HIRSCHMANN
A BELDEN BRAND

User Manual

Configuration
Lite Managed Switch
GECKO 8TX/2SFP

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

© 2024 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use.

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

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

You can get the latest version of this manual on the Internet at the Hirschmann product site (www.hirschmann.com).

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

Contents

Safety instructions

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.

Warranty regarding further use of the Open Source Software

Hirschmann Automation and Control GmbH provides no warranty for the Open Source Software contained in this product, if such Open Source Software is used in any manner other than intended by Hirschmann Automation and Control GmbH. The licenses listed below define the warranty, if any, from the authors or licenser of the Open Source Software. Hirschmann Automation and Control GmbH specifically disclaims any warranty for defects caused by altering any Open Source Software or the product's configuration. Any warranty claims against Hirschmann Automation and Control GmbH in the event that the Open Source Software contained in this product infringes the intellectual property rights of a third party are excluded.

The following disclaimer applies to the GPL and LGPL components in relation to the rights holders:
“This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License and the GNU Lesser General Public License for more details.”

For the remaining open source components, the liability exclusions of the rights holders in the respective license texts apply.

Technical support, if any, will only be provided for unmodified 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.

About this Manual

The documentation for your device is made up of the following documents.

Mounting instructions	This document contains safety instructions and information that you need for mounting the device.
Installation user manual	This document contains a device description, safety instructions and further information that you need for installing the device before you start configuring it.
Configuration user manual	This document contains the information that you need for starting up the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.
Online help	The online help contains descriptions of the individual parameters that you configure via the graphical user interface.Use the “Help” button to call up the online help in the graphical user interface. The content of the online help corresponds to the information in the “References” chapter of the configuration user manual.

You can find the documentation that is not provided as a printout with your device as a PDF file under “Downloads” at www.hirschmann.com/de/QR/INET-GECKO8TX_de-HB.
The Network Management Software Industrial HiVision provides you with options for smooth configuration and monitoring. You find further information on the Internet at the Hirschmann product pages:
http://www.hirschmann.com/en/QR/INET-Industrial-HiVision

Key

Designations used:

▶	List
☐	Work step
■	Subheading
Link	Cross-reference with link
Note:	A note emphasizes an important fact or draws your attention to a dependency.
`Courier`	ASCII representation in user interface

Introduction

The device has been developed for use in a harsh industrial environment. Accordingly, the installation process has been kept simple. Thanks to the selected default settings, you only have to enter a few settings before starting to operate the device.

Note: The device saves changed settings in the temporary memory when you click "Set".
You use the `Basic Settings > Load/Save` dialog to save changed settings in the local memory of the device.

1 Defining IP parameters

Note: You will find background information on this topic here: “IP Parameter Basics” on page 145.

To access the device via the network during the first installation, you require the IP parameters of the device.

The device gives you the following options for defining IP parameters:

- Defining IP Parameters via DHCP (state on delivery)
  You need a DHCP server for this. The DHCP server assigns the IP parameters to the device using its MAC address or its system name.

- Defining IP Parameters via HiDiscovery
  You choose this method on a previously installed network device or if you have another Ethernet connection between your PC and the device.

- Defining IP Parameters via BOOTP
  You need a BOOTP server for this method. The BOOTP server assigns the IP parameters to the device using its MAC address.

- Defining IP parameters via the graphical user interface
  You choose this method if your device already has an IP address and can be accessed via the network.

1.1 Defining IP Parameters via DHCP (state on delivery)

Note: You will find background information on this topic here: “Basics of the Dynamic Host Configuration Protocol (DHCP)” on page 151.

Prerequisite:

- You need a DHCP server. The DHCP server assigns the configuration data to the device using its MAC address or its system name.

On delivery, the definition of the IP parameters via a DHCP server is activated. The device tries to obtain an IP address from a DHCP server.

If there is no response from the DHCP server, the device sets the IP address to 0.0.0.0 and makes another attempt to obtain a valid IP address.

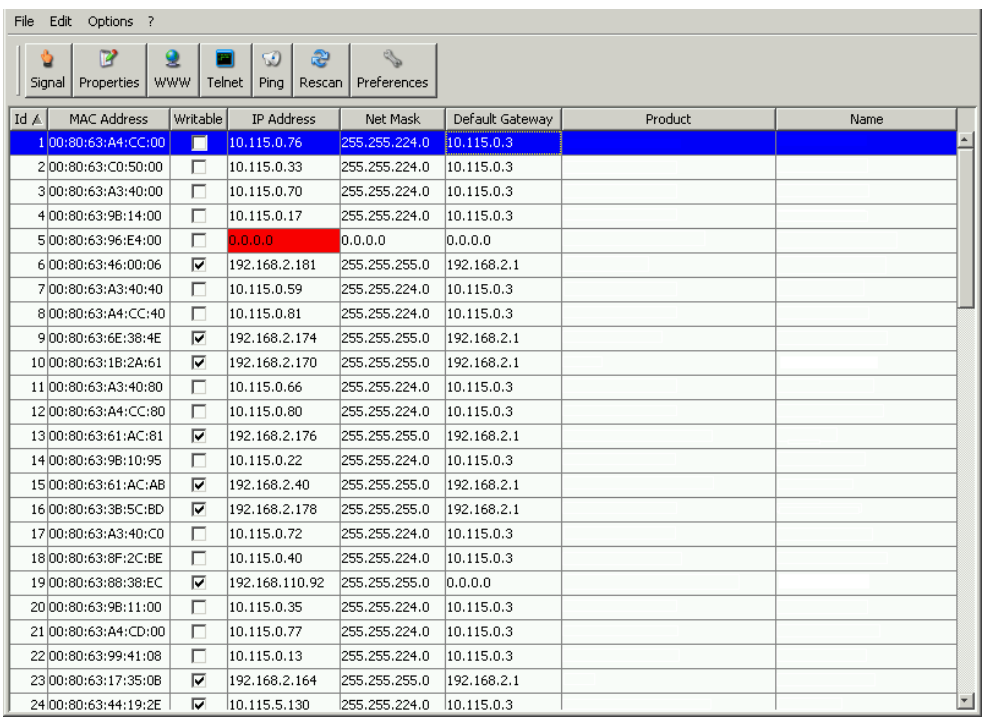
To activate or deactivate the definition of the IP parameters via a DHCP server, you change the source from which the device obtains its IP parameters in the `Basic Settings > Network` dialog, "Management Interface" frame.

1.2 Defining IP Parameters via HiDiscovery

The HiDiscovery protocol enables you to assign IP parameters to the device via the Ethernet.

Install the HiDiscovery software on your PC. You can download the software from the Hirschmann product pages.

☐ Start the HiDiscovery program.



Id	MAC Address	Writable	IP Address	Net Mask	Default Gateway	Product	Name
1	00:80:63:A4:CC:00	☐	10.115.0.76	255.255.224.0	10.115.0.3		
2	00:80:63:C0:50:00	☐	10.115.0.33	255.255.224.0	10.115.0.3		
3	00:80:63:A3:40:00	☐	10.115.0.70	255.255.224.0	10.115.0.3		
4	00:80:63:9B:14:00	☐	10.115.0.17	255.255.224.0	10.115.0.3		
5	00:80:63:96:E4:00	☐	0.0.0.0	0.0.0.0	0.0.0.0		
6	00:80:63:46:00:06	☑	192.168.2.181	255.255.255.0	192.168.2.1		
7	00:80:63:A3:40:40	☐	10.115.0.59	255.255.224.0	10.115.0.3		
8	00:80:63:A4:CC:40	☐	10.115.0.81	255.255.224.0	10.115.0.3		
9	00:80:63:6E:38:4E	☑	192.168.2.174	255.255.255.0	192.168.2.1		
10	00:80:63:1B:2A:61	☑	192.168.2.170	255.255.255.0	192.168.2.1		
11	00:80:63:A3:40:80	☐	10.115.0.66	255.255.224.0	10.115.0.3		
12	00:80:63:A4:CC:80	☐	10.115.0.80	255.255.224.0	10.115.0.3		
13	00:80:63:61:AC:81	☑	192.168.2.176	255.255.255.0	192.168.2.1		
14	00:80:63:9B:10:95	☐	10.115.0.22	255.255.224.0	10.115.0.3		
15	00:80:63:61:AC:AB	☑	192.168.2.40	255.255.255.0	192.168.2.1		
16	00:80:63:3B:5C:BD	☑	192.168.2.178	255.255.255.0	192.168.2.1		
17	00:80:63:A3:40:C0	☐	10.115.0.72	255.255.224.0	10.115.0.3		
18	00:80:63:8F:2C:BE	☐	10.115.0.40	255.255.224.0	10.115.0.3		
19	00:80:63:88:38:EC	☑	192.168.110.92	255.255.255.0	0.0.0.0		
20	00:80:63:9B:11:00	☐	10.115.0.35	255.255.224.0	10.115.0.3		
21	00:80:63:A4:CD:00	☐	10.115.0.77	255.255.224.0	10.115.0.3		
22	00:80:63:99:41:08	☐	10.115.0.13	255.255.224.0	10.115.0.3		
23	00:80:63:17:35:0B	☑	192.168.2.164	255.255.255.0	192.168.2.1		
24	00:80:63:44:19:2E	☑	10.115.5.130	255.255.224.0	10.115.0.3		

Figure 1: 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. If your computer has several network cards, you can select the one you desire in the HiDiscovery toolbar.

HiDiscovery displays a line for every device that reacts to the HiDiscovery protocol.

HiDiscovery enables you to identify the devices displayed.

- ☐ Select a device line.
- ☐ Click the "Signal" symbol in the tool bar to set the LEDs for the selected device flashing. To switch off the flashing, click on the symbol again.
- ☐ By double-clicking a line, you open a window in which you can enter the device name and the IP parameters.

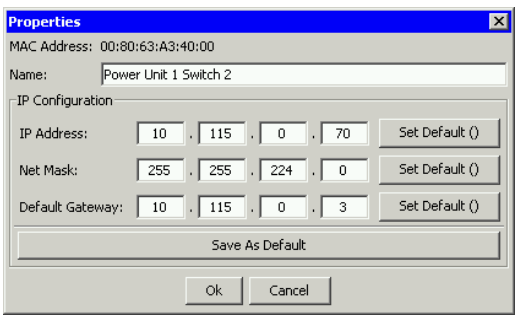


Figure 2: HiDiscovery – IP parameter assignment

Note: For security reasons, switch off the HiDiscovery function for the device in the graphical user interface, after you have assigned the IP parameters to the device.
See “Enabling/disabling HiDiscovery access” on page 46.

Note: So that the entries are available again after a restart, you save the settings in the local non-volatile memory of the device via the "Load/Save" dialog.

1.3 Defining IP parameters via the graphical user interface

Prerequisite:

- Your device already has an IP address and can be accessed via the network.

Procedure:

☐ Open the `Basic Settings > Network` dialog.

☐ In the "IP Parameters" frame, define the IP parameters of the device:

Parameter	Meaning
IP Address	Specifies the IP address under which the device management can be accessed via the network. Possible values: ▶ Valid IPv4 address (default setting: —)
Netmask	Specifies the netmask. The netmask identifies the network prefix and the host address of the device in the IP address. Possible values: ▶ Valid IPv4 netmask (default setting: —)
Gateway address	Specifies the IP address of a router through which the device accesses other devices outside its own network. Possible values: ▶ Valid IPv4 address (default setting: —)

☐ To temporarily save the changes, click "Set".

Note: So that the entries are available again after a restart, you save the settings in the local non-volatile memory of the device via the "Load/Save" dialog.

1.4 Defining IP Parameters via BOOTP

Prerequisite:

- You need a BOOTP server for this method. The BOOTP server assigns the configuration data to the device using its MAC address.

Procedure:

☐ Open the `Basic Settings > Network` dialog.

☐ To activate the assignment of the IP parameters via a BOOTP server, select the `BOOTP` value in the "Management Interface" frame.

With the BOOTP function activated the device sends a boot request message to the BOOTP server. The server answers with a boot reply message. The boot reply message contains the assigned IP address.

If there is no response from the BOOTP server, the device sets the IP address to 0.0.0.0 and makes another attempt to obtain a valid IP address.

2 Access to the device

2.1 First login (Password change)

To help prevent undesired access to the device, it is imperative that you change the default password during initial setup.

The device offers you the following methods for changing the password:

- ☐ Open the Graphical User Interface, or the Command Line Interface, the first time you log on to the device.
- ☐ Log on to the device with the default password.
  The device prompts you to type in a new password.
- ☐ Type in your new password.
  To help increase security, choose a password that contains at least 8 characters which includes upper-case characters, lower-case characters, numerical digits, and special characters
- ☐ Confirm your new password
- ☐ Click the OK button.
- ☐ The device displays a dialog that informs you that the password has changed. Click the OK button.
- ☐ Log on to the device again with your new password

Parameter	Meaning
Password	The default password is `private`.
New Password (1)	Type in your new password. Create a password that contains at least 8 characters. The exception to this rule is `private` and `public`. Possible values: ▶ a-z, A-Z ▶ #$%&#()*+,-./:;<=>?@[]^_‘{}~!|
New Password (2)	Confirm your new password
Language	Select the dialog language.

For further information see:https://hirschmann-support.belden.com

Figure 3: First Login Dialog

The following tables list the default settings of the protocols.

Note: The SSH protocol is only enabled for the initial password change. After you change the password, the device disables the ssh protocol.

Protocol	Default setting
SNMP v1	Disabled
SNMP v2	Disabled
SNMP v3	Disabled
CLI SSH	Enabled
CLI Telnet	Disabled
CLI V.24/USB	Enabled
MOPS BASIC Auth	Disabled
MOPS MOPS Auth	Enabled
HTTP(S)	Enabled
DHCP	Enabled
SNMP over HTTP(S)	Enabled

Table 1: Management protocols

Protocol	Default setting
Transferclients (TFTP, SFTP, SCP)	Enabled
Transfer Server (SCP)	Disabled

Table 2: File transfer protocols

Note: Using the options 66 - TFTP Server Name and option 67 - Bootfile Name bring risks. The device sends unauthenticated DHCP client messages to a server using User Datagram Port (UDP) 67. The messages are broadcast messages, meaning that everyone can receive the messages and anyone can respond to the messages.

Protocol	Default setting
Profinet	Disabled

Table 3: Industrial protocols

2.2 Starting the graphic user interface

Prerequisite:

▶ The IP parameters of the device are defined and the device can be accessed via the network.
See “Defining IP parameters” on page 17.

Procedure:

☐ Start your Web browser.

Note: This device does not support Windows Internet Explorer v11 and earlier.

☐ Write the IP address of the device in the address field of the Web browser. Use the following format: `https://xxx.xxx.xxx.xxx`

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

☐ Select the language for the graphical user interface.
☐ Select the user name and the password:
☐ Click "OK".
The Web browser shows the window with the graphical user interface.

3 Loading/Storing the Configuration

The device gives you the following options for loading or saving the device configuration:

- Resetting the configuration to the delivery state
- Importing a configuration
- Saving the configuration in the device
- Exporting a configuration

Note: The device saves changed settings in the temporary memory when you click "Set".
You use the `Basic Settings > Load/Save` dialog to save changed settings in the local memory of the device.

3.1 Resetting the configuration to the delivery state

When it is restarted, the device loads its configuration data from the local non-volatile memory.
If you reset the settings in the device to the delivery state, the device deletes the configuration in the volatile memory and in the non-volatile memory. The device then reboots and loads the delivery settings.

Prerequisite:
- ▶ You are accessing the device as an “admin” user with read and write access.

Procedure:
- ☐ Select the dialog `Basic Settings > Load/Save`.
- ☐ In the "Load/Save" frame, click the "Reset" button beside “Back to delivery state”.

3.2 Importing a configuration

The device allows you to load settings from a configuration file from your PC or from a TFTP server.

Prerequisite:
- You are accessing the device as an “admin” user with read and write access.
- Import from a TFTP server
  The configuration file is saved in the relevant path of the TFTP server with the file name, e.g. `backup/config.bin`
  See “Exporting a configuration” on page 34.
- Import from your PC:
  The configuration file is saved as a binary file on your PC.

Procedure:
☐ Select the dialog `Basic Settings > Load/Save`.
☐ Select the `Server to device` value for the transfer direction in the "Configuration Transfer"frame.
  - Or enter the path for the configuration file on a TFTP server.
    The URL identifies the path to the configuration file saved on the TFTP server with the file name. The URL has the form tftp://IP address of the TFTP server/path name/file name.
  - Or use Drag & Drop to pull the file to the dotted area in the “Configuration Transfer” frame.
    This option support the common Web browsers except the Internet Explorer.

☐ Click "Transfer".
  After the update is completed successfully, you activate the configuration: Restart the device by clicking “Restart”.

Note: Loading a configuration deactivates the ports while the configuration is being set up. Afterwards, the device sets the port status according to the new configuration.

Note: The device saves changed settings in the temporary memory when you click "Set".
You use the `Basic Settings > Load/Save` dialog to save changed settings in the local memory of the device.

3.3 Saving the configuration in the device

The device allows you to save the current configuration data in the local non-volatile memory of the device.

Prerequisite:

- You are accessing the device as an “admin” user with read and write access.

Procedure:

☐ Select the dialog `Basic Settings > Load/Save`.

☐ In the "Load/Save" frame, click the "Save" button beside "Save current configuration".

3.4 Exporting a configuration

The device allows you to save settings in a configuration file on your PC or on a TFTP server.

Prerequisite:
- You are accessing the device as an “admin” user with read and write access.

Procedure:
☐ Select the dialog `Basic Settings > Load/Save`.
☐ Select the `Device to server` value for the transfer direction in the "Configuration Transfer" frame.
  - Either click "Download" beside "Save as" in the "Configuration Transfer" frame to save the configuration on your PC.
  - Or enter the path to the storage location on a TFTP server.
    The URL identifies the path to the configuration file saved on the TFTP server with the file name. The URL has the form
    tftp://IP address of the TFTP server/path name/file name.
    Click "Transfer".

Note: The device saves changed settings in the temporary memory when you click "Set".
You use the `Basic Settings > Load/Save` dialog to save changed settings in the local memory of the device.

4 Checking the status of the software/updating the software

Hirschmann never stops working on improving the performance of its products. So it is possible that you may find a more up to date release of the software on the Hirschmann Internet site (www.hirschmann.com) than the release saved on your device.

4.1 Checking the status of the software

The device allows you to display the status of the software saved on the device.

Procedure:
☐ Select the `Basic settings > Software` dialog.
☐ The "Running Version" frame shows you the release number of the software saved on the device.

4.2 Updating the software

Prerequisite:

- The file with the more recent software version is saved on a TFTP server, on your PC or on a network drive.

Procedure:

☐ Select the `Basic settings > Software` dialog.

You have 2 options for updating the software:

- Enter the path for the configuration file on a TFTP server.
  The URL identifies the path to the software saved on the TFTP server with the file name. The URL has the form
  tftp://IP address of the TFTP server/path name/file name.
- Or use Drag & Drop to pull the file to the dotted area in the “software update” frame.
  This option support the common Web browsers except the Internet Explorer.

☐ Click "Install" to transfer the software to the device.
The “Status” frame shows the progress of the installation.
After a successful installation, the message “Flash 100.00 % completed” appears in the progress bar.

☐ After successfully loading it, you activate the new software:
Restart the device by clicking “Restart”.

5 Configuring the Ports

This device gives you the following options for defining basic settings for the ports:

- Enabling/disabling ports
  For a higher level of access security, disable the ports at which you are not connecting any other network components.

- Selecting the operating mode
  The device allows you to manually select the data transfer rate and a half duplex or full duplex connection, or to have the device define this automatically (autonegotiation).

- Switching link monitoring (alarm messages) on/off
  The device allows you to transfer alarm messages to a network management station.

5.1 Enabling/disabling ports

Every port is enabled in the state on delivery. For a higher level of access security, disable the ports at which you are not connecting any network components.

Procedure:

☐ Select the dialog `Basic Settings > Port > Configuration`.

☐ To enable or disable a port, select the value `Off` or `On` in the "State" column for the relevant port.

Note: The device saves changed settings in the temporary memory when you click "Set".
You use the `Basic Settings > Load/Save` dialog to save changed settings in the local memory of the device.

5.2 Selecting the operating mode

In the state on delivery, the ports are in the "autonegotiation" operating mode.

With autonegotiation, the device autonomously determines the maximum possible data transfer rate and the duplex mode between the connected ports.

If autonegotiation is switched off at the remote site, the device uses the “parallel detection” method. The device determines the maximum possible data transfer rate and selects the half duplex mode. Set the remote site to half duplex, as otherwise the result is a duplex mismatch (one side supports full duplex and the other supports half duplex). This causes a very slow connection.

Procedure:

☐ Select the dialog `Basic Settings > Port > Configuration`.

☐ If the device connected to this port requires a fixed setting, select the transfer speed and the duplex mode in the "Manual Configuration" column.

Note: The device saves changed settings in the temporary memory when you click "Set".
You use the `Basic Settings > Load/Save` dialog to save changed settings in the local memory of the device.

5.3 Switching link monitoring (alarm messages) on/off

The device allows you to transfer alarm messages to a network management station. In the `Basic Settings > Port > Configuration` dialog, you specify whether the device sends an SNMP trap when it detects a change in the monitored functions. You specify the monitored functions in the `Diagnostics > Alarms (Traps)` dialog.

Procedure:

☐ Select the dialog `Basic Settings > Port > Configuration`.

☐ To enable or disable the transfer of alarm messages to a network management station, select the value `On` or `Off` in the "Link Monitoring" column for the relevant port.

☐ To save the changed settings in the temporary memory of the device, click "Set".

Note: The device saves changed settings in the temporary memory when you click "Set".
You use the `Basic Settings > Load/Save` dialog to save changed settings in the local memory of the device.

6 Helping prevent unauthorized access

The device provides you with the following options to help you protect it against unauthorized access.

- Changing passwords
  For a higher level of access security, change the preset passwords for the access to the device.

- Enabling/disabling ports
  Disable the ports on which you are not connecting any other network components.

- Enabling/disabling HiDiscovery access
  Restrict the HiDiscovery function for the device or disable it after you have assigned the IP parameters to the device.

- Adjusting the SNMP access
  To make unauthorized access to the device more difficult, change the community for read/write access, define a different community for read/write access than for read access, and only use SNMPv1 or SNMPv2 in environments protected from eavesdropping. We recommend using SNMPv3 and deactivating the access via SNMPv1 and SNMPv2 in the device.

6.1 Changing passwords

Note: The passwords for accessing the device via the graphical user interface are the same as the passwords for accessing the device via SNMPv3.

A network management station communicates with the device via the Simple Network Management Protocol (SNMP).
Every SNMP packet contains the IP address of the sending computer and the password with which the sender of the packet wants to access the management information base (MIB) of the device.

The device receives the SNMP packet and compares the IP address of the sending computer and the password with the entries in the MIB of the device. If the password has the appropriate access rights, and if the IP address of the sending computer has been entered, the device will allow access.

Prerequisite:

▶ You are accessing the device as an “admin” user with read and write access.

Please note the following information on passwords:

☐ Define a new password with which you can access from your computer with write access.
Treat this community with discretion since everyone who knows the password can access the MIB of the device with the IP address of your computer.

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

Procedure:

☐ Select the `Device Security > Password` dialog.
☐ Select "Modify read-only password (user)" to enter the read password or "Modify read/write password (admin)" to enter the read/write password. The minimum password length is 8 characters. Upper- and lower-case letters, numbers and special characters are allowed.
☐ Enter the password for user “admin” in the "Current Administrator Password" field.
☐ Enter the new password in the "New Password" field.
☐ Repeat your entry in the "Please retype" field.
☐ To save the changed settings in the temporary memory of the device, click "Set".

Note: So that the entries are available again after a restart, you save the settings in the local non-volatile memory of the device via the "Load/Save" dialog.

6.2 Enabling/disabling HiDiscovery access

The HiDiscovery protocol enables you to assign IP parameters to the device via the Ethernet.
You will find more information on this topic here: “Defining IP Parameters via HiDiscovery” on page 19.

Note: Restrict the HiDiscovery function for the device or disable it after you have assigned the IP parameters to the device.

Procedure:
- ☐ Select the `Basic Settings > Network` dialog.
- ☐ To disable the HiDiscovery function, select the value `Off` for "Operation" in the "HiDiscovery Protocol" frame.
- ☐ To disable the write access to the device using HiDiscovery, select the value `Off` for "Write Permission" in the "HiDiscovery Protocol" frame.
- ☐ To save the changed settings in the temporary memory of the device, click "Set".

Note: The device saves changed settings in the temporary memory when you click "Set".
You use the `Basic Settings > Load/Save` dialog to save changed settings in the local memory of the device.

6.3 Adjusting the SNMP access

The SNMP protocol allows you to monitor and configure the device via the network with a network management system (NMS). When the NMS accesses the device via SNMPv1 or SNMPv2, the NMS authenticates itself with the community. When the NMS accesses the device via SNMPv3, the NMS authenticates itself with a user's login data.

Make the following basic provisions to make undesired access to the device more difficult:

- ☐ Change the community for read/write access. Treat this community confidentially. Everyone who knows the community has the option to change the settings for the device.
  See "Modifying the community for read/write access" on page 48.
- ☐ Specify a different community for read/write access than for read access.
  See "Modifying the community for read/write access" on page 48.
- ☐ Use SNMPv1 or SNMPv2 only in environments protected from eavesdropping. The protocols do not use encryption. The SNMP packets contain the community in clear text. We recommend using SNMPv3 and deactivating the access via SNMPv1 and SNMPv2 in the device.
  See "Deactivating the access via SNMPv1 or SNMPv2 in the device" on page 49.
  See "Activating access via SNMPv3 in the device" on page 49.

6.3.1 Modifying the community for read/write access

In the state on delivery, you access the device via the communities public (read access) and private (read/write access).

The community is contained in every SNMP packet. When it receives a packet, the device compares this community with the communities specified in the device. If the communities match, the device accepts the SNMP packet and grants access.

Prerequisite:

- You are accessing the device as an “admin” user with read and write access.

Procedure:

☐ Open the `Device Security > SNMP` dialog.
The dialog shows the communities that are set up.

☐ In the row for the `Write` community, click the "Name" field. Enter the community.
- Up to 32 alphanumeric characters are allowed.
- The device differentiates between upper and lower case.
- Specify a different community than for read access.

☐ To save the changed settings in the temporary memory of the device, click "Set".

Note: The device saves changed settings in the temporary memory when you click "Set".
You use the `Basic Settings > Load/Save` dialog to save changed settings in the local memory of the device.

6.3.2 Deactivating the access via SNMPv1 or SNMPv2 in the device

Prerequisite:

- You are accessing the device as an “admin” user with read and write access.

Procedure:

☐ Open the `Device Security > SNMP` dialog.
☐ To deactivate the SNMPv1 protocol, you remove the selection from the "SNMPv1 enabled" checkbox.
☐ To deactivate the SNMPv2 protocol, you remove the selection from the "SNMPv2 enabled" checkbox.
☐ To save the changed settings in the temporary memory of the device, click "Set".

Note: The device saves changed settings in the temporary memory when you click "Set".
You use the `Basic Settings > Load/Save` dialog to save changed settings in the local memory of the device.

6.3.3 Activating access via SNMPv3 in the device

Prerequisite:

- You are accessing the device as an “admin” user with read and write access.

Procedure:

☐ Open the `Device Security > SNMP` dialog.
☐ To activate the SNMPv3 protocol, select the "SNMPv3 enabled" checkbox.
☐ To save the changed settings in the temporary memory of the device, click "Set".

Note: The device saves changed settings in the temporary memory when you click "Set".
You use the `Basic Settings > Load/Save` dialog to save changed settings in the local memory of the device.

7 Network load control

The device gives you the following options for reducing the network load:

- Direct packet distribution
- Prioritizing the data traffic (Quality of Service)

7.1 Direct packet distribution

The device reduces the network load with direct packet distribution.

The device learns the MAC address of the senders of received data packets at every port. The device saves the combination “port and MAC address” in a 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 defective data packets.

7.1.1 Learning MAC addresses

If the device receives a data packet, it checks whether the MAC address of the sender is already saved in the MAC address table. If the MAC address of the sender is unknown, the device generates a new entry. The device then compares the destination MAC address of the data packet with the entries saved in the MAC address table:

- The device sends 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.

7.1.2 Aging of learned MAC addresses

Addresses that have not been detected by the device for the period of time of 30 seconds (aging time) are deleted from the MAC address table (FDB) by the device. A reboot or resetting of the MAC address table deletes the entries in the MAC address table (FDB).

7.1.3 Creating static address entries

In addition to learning the sender MAC address, the device also provides the option to set MAC addresses manually. These MAC addresses remain configured and survive resetting of the MAC address table as well as rebooting of the device.

Static address entries allow the device to forward data packets directly to selected device ports.

Prerequisite:

▶ You are accessing the device as an “admin” user with read and write access.

Procedure:

☐ Open the `Switching > Filter for MAC addresses` dialog.
☐ To add a user-defined MAC address, click "Create".
☐ In the "Address" field, define the destination MAC address to which the table entry applies.
☐ In the "Possible Ports" field, select the device ports to which the device sends data packets with the specified destination MAC address.
  ☐ Select exactly one device port if you have defined a unicast MAC address in the "Address" field.
  ☐ Select one or more device ports if you have defined a multicast MAC address in the "Address" field.
☐ Click "OK".
☐ To save the changed settings in the temporary memory of the device, click "Set".

Note: The device saves changed settings in the temporary memory when you click "Set".
You use the `Basic Settings > Load/Save` dialog to save changed settings in the local memory of the device.

7.1.4 Deleting learned address entries

Prerequisite:
- ▶ You are accessing the device as an “admin” user with read and write access.

Procedure:
- ☐ To delete the learned addresses from the MAC address table (FDB), open the `Switching > Filter for MAC Addresses` dialog and click the "Delete" button beside the address entry to be deleted.
- ☐ To save the changed settings in the temporary memory of the device, click "Set".

Note: The device saves changed settings in the temporary memory when you click "Set".
You use the `Basic Settings > Load/Save` dialog to save changed settings in the local memory of the device.

7.2 Prioritizing the data traffic (Quality of Service)

Note: You will find background information on this topic here: “Basics of the Spanning Tree Protocol” on page 153.

QoS (Quality of Service) is a procedure defined in IEEE 802.1D. It is used to distribute resources in the network. QoS allows you to prioritize the data of specific applications.

Prioritizing helps prevent data traffic with lower priority from interfering with delay-sensitive data traffic, especially when there is a heavy network load. Delay-sensitive data traffic includes, for example, voice, video, and real-time data.

7.2.1 Setting prioritization

■ Assigning the port priority

- ☐ Open the `Switching > QoS/Priority > Port Configuration` dialog.
- ☐ In the "Port Priority" column, you define the priority with which the device sends the data packets received on this port without a VLAN tag.
- ☐ In the "Trust Mode" column, you define the criteria the device uses to assign a traffic class to data packets received.
- ☐ To save the changed settings in the temporary memory of the device, click "Set".

Assigning VLAN priority to a traffic class

- ☐ 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.
- ☐ To save the changed settings in the temporary memory of the device, click "Set".

Assigning DSCP to a traffic class

- ☐ Open the `Switching > QoS/Priority > IP DSCP Mapping` dialog.
- ☐ Enter the desired value in the "Traffic Class" column.
- ☐ To save the changed settings in the temporary memory of the device, click "Set".

Note: The device saves changed settings in the temporary memory when you click "Set".
You use the `Basic Settings > Load/Save` dialog to save changed settings in the local memory of the device.

8 Diagnostics

The device provides you with the following diagnostic tools:

- Setting alarms (traps)
- Displaying the topology discovery
- System log

8.1 Setting alarms (traps)

The device immediately reports unusual events which occur during normal operation to the management station. This is done by messages called traps that bypass the polling procedure (“polling” means querying the data stations at regular intervals). Traps allow you to react quickly to unusual events.

The device sends traps to those hosts entered in the trap destination table. The device allows you to configure the trap destination table with the management station via SNMP.

List of SNMP traps

The following table shows a list of possible traps sent by the device.

Name of the trap	Meaning
authenticationFailure	is sent if a station attempts to access an agent without permission.
coldStart	is sent during the boot phase when a cold start is performed (after the successful initialization of the network management).
linkDown	is sent if the link to a port is interrupted.
linkUp	is sent when the connection to a port is intact.
lldpRemTablesChange	is sent if an entry in the topology table is changed.
newRoot	is sent if the sending agent becomes a new root of the spanning tree.
topologyChange	is sent if the port status changes from “blocking” to “forwarding”, or from “forwarding” to “blocking”.

Table 4: Possible traps

Prerequisite:

▶ You are accessing the device as an “admin” user with read and write access.

Procedure:

☐ Open the `Diagnostics > Alarms (traps)` dialog.

This dialog allows you to specify which events trigger a trap, and where the device sends these messages.

☐ In the "Destination Addresses" frame you enter the name of the trap community that the device uses to identify itself as the source of the trap.

☐ Enter the IP address of the management stations to which the device sends the traps.

The device generates traps for changes that have been selected in the `Alarms (traps)` frame. Create at least one SNMP manager that receives traps.

8.2 Displaying the topology discovery

Note: You will find background information on this topic here: “Basics of the Topology Discovery” on page 172.

Procedure:
☐ Open the `Diagnostics > LLDP` dialog.

The “Topology Discovery” frame displays the collected LLDP information for the neighboring devices. This information enables the network management station to map the structure of your network.

Parameter	Meaning
Port	Displays the number of the device port.
Neighbor Identifier	Displays the chassis ID of the neighboring device. This can be the basis MAC address of the neighboring device, for example.
Neighbor IP Address	Displays the IP address with which the management functions of the neighboring device can be reached.
Neighbor Port Description	Displays a description for the device 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.

If you use a port to connect several devices, for example via a hub, the table contains a line for each connected device.

The FDB address table contains MAC addresses of devices that the topology table hides for the sake of clarity.

8.3 System log

The system log file is an HTML file in which the device writes every specific device-internal event. In service situations, this report provides the necessary information to the technician.

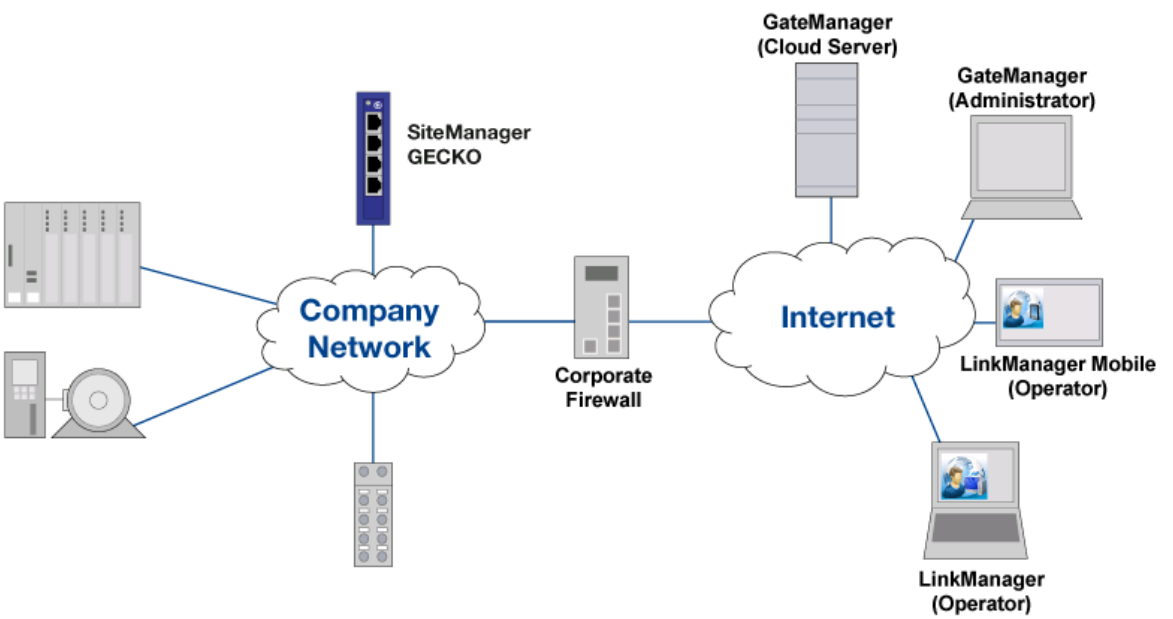
The table in the `Diagnostics > System Log` dialog lists the logged events.
☐ To archive the content of the log as an HTML file, click the “Save” button.

9 Support in Secure Remote Access

In combination with the SiteManager GECKO, the device offers you a tool which assists you with a Secure Remote Access.

Secure Remote Access allows you to do the following:

- Connect devices which are located geographically away from each other.
- Remote programming of industrial components using familiar tools.
- Remote control and remote monitoring of industrial plants using your PC, iPhone or Android device.
- Operating machines without physical access to the network in which the machine is located.
- Applying secure mechanisms on devices which usually are classified as unsecure (tablets or smartphones).
- Creating accounts for machine operators with separate accounts to specific devices.



9.1 SiteManager GECKO

The SiteManager GECKO is a Hirschmann client which supports Secure Remote Access. It helps to build up secure connections of up to 10 devices which are connected to the SiteManager GECKO.

The dialog allows you to do the following:
- Specify basic settings for the SiteManager GECKO.
- Control the connection status to the GateManager Server and display the software version of the client.
- Reset the SiteManager GECKO Client to the default settings.
- Save a log file on the PC.

9.1.1 Configuring the SiteManager GECKO

Prerequisite:
- You are accessing the device as an “admin” user with read and write access.

Procedure:
☐ Open the dialog `Secure Remote Access > SiteManager GECKO`.

☐ In the "Configuration" frame next to “Operation”, mark the “On” checkbox to enable the function.

☐ In the "Configuration" frame, specify the following values:
- “GateManager Server” field: IPv4 address of the GateManager Server.
- “GateManager Token” field: Domain token for the connection to the GateManager GECKO.
- “Name” field: Name which is describing the SiteManager GECKO.

The device starts setting up the connection from the SiteManager GECKO to the GateManager. The "Status" frame displays the status of the connection.

Configuration

Description	Meaning
Operation	When the function is on, the device initiates a connection to the GateManager. Possible values: ▶ “On“ The SiteManager GECKO initiates a permanent connection to the GateManager using the specified values. ▶ “Off“ (default setting) No connection to the GateManager.
GateManager Server	Specifies the IPv4 address of the GateManager Server. Possible values: ▶ Valid IPv4 address If the specified IP address in the configured subnet is unreachable, use a webproxy or a gateway. The "Basic Settings" > "Network” dialog, “IP Parameter” frame, “Gateway Address” field allows you to specify the gateway. Alternatively, you specify the gateway using HiDiscovery or a DHCP server. The “Webproxy Address”, “Webproxy Account” and “Webproxy Password” fields allow you to specify the data for the webproxy.
GateManager Token	Specifies the domain token for connecting to the GateManager GECKO. Possible values: ▶ Alphanumeric ASCII character string
Name	Specifies the description for the entry. Enter a name to describe the SiteManager GECKO. Possible values: ▶ Alphanumeric ASCII character string
Webproxy Address	Specifies the IPv4 address for the webproxy. Possible values: ▶ `[blank]` No webproxy. ▶ Valid IPv4 address Use a gateway, if the webproxy and GECKO are located in different subnets.
Webproxy Account	Specifies the user name with which the user authenticates on the webproxy.
Webproxy Password	Specifies the password with which the user authenticates on the webproxy.

Table 5: Configuration

Status

Description	Meaning
Status	Displays the connection status between the SiteManager GECKO and the GateManager. Possible values: ▶ `Starting` The device initiates the connection. The SiteManager GECKO verifies the validity of the GateManager's IP address. ▶ `Not connected` Connection between SiteManager GECKO and GateManager inactive. ▶ `Conncting to a.b.c.d` The device tries to establish the connection from the SiteManager GECKO to the GateManager. If you are using a webproxy, the device tries to establish the connection to the GateManager using the webproxy. ▶ `Connected to a.b.c.d` Connection between SiteManager GECKO and GateManager active.

Table 6: Status

SiteManager GECKO

Description	Meaning
Running Version	Displays the version number of the SiteManager GECKO that the device is currently running. The GateManager allows you to update the SiteManager GECKO only. The "Software Update" frame in the "Basic Settings" > "Software" dialog allows you to update the GECKO device software and the SiteManager simultaneously. See "Updating the software" on page 37

Table 7: SiteManager GECKO

Buttons

Reset	Reset SiteManager GECKO to factory default Resets the SiteManager GECKO to factory default. The device overwrites the updates which you have installed using the GateManager. The GECKO device software remains unmodified. You reset the complete GECKO device software, using the "Reset" button next to "Back to factory defaults" located in the "Basic Settings > Load/Save" dialog in the "Load/Save" frame.
Save	SiteManager GECKO Log Saves the "sitemanager_syslog0.txt" log file on your PC. The file contains detailed information about connections and run-time status.
Reload	Updates the fields with the values that are saved in the volatile memory(RAM) of the device.
Set	Transfers the changes to the volatile memory (RAM) of the device andapplies them to the device. To save the changes in the non-volatilememory, proceed as follows: ☐ Open`Basic Settings > Load/Save` dialog. ☐ Click the "Save" button in the "Load/Save" frame next to "Save current configuration".
Help	Opens the online help.

10 Configuring the Rapid Spanning Tree Protocol redundancy procedure

Note: You will find background information on this topic here: “Basics of the Spanning Tree Protocol” on page 153.

The device supports the Rapid Spanning Tree Protocol (RSTP) defined in standard IEEE 802.1D-2004. This protocol is a further development of the Spanning Tree Protocol (STP) and is compatible with it.

The Rapid Spanning Tree Protocol enables fast switching to a newly calculated topology without interrupting existing connections.
RSTP configures the network topology completely independently. The device with the lowest bridge priority automatically becomes the root bridge. However, to define a specific network structure regardless, you specify a device as the root bridge. In general, a device in the backbone takes on this role.

Procedure:

☐ Set up the network to meet your requirements, initially without redundant lines.

☐ Switch Spanning Tree on every device in the network.
In the state on delivery, Spanning Tree is switched on the device.
  ☐ Open the `Redundancy > Spanning Tree > Global` dialog.
  ☐ In the "Operation" frame, select the value `On`.

☐ Click “Set“ to save the changes.

☐ You now connect the redundant lines.

☐ Define the settings for the device that takes over the role of the root bridge.

☐ In the “Priority“field you enter a numerically lower value.
The bridge with the numerically lowest bridge ID has the highest priority and becomes the root bridge of the network.

☐ Click “Set“ to save the changes.

☐ If applicable, change the values in the “Forward Delay [s]“ and “Max Age“ fields.

☐ Click “Set“ to save the changes.

Note: The parameters “Forward Delay [s]“ and “Max Age“ have the following relationship:
“Forward Delay [s]“ ≥ (“Max Age“/2) + 1
If you enter values in the fields that contradict this relationship, the device replaces these values with the last valid values or with the default value.

☐ Check the following values in the other devices:
  – Bridge ID (bridge priority and MAC address) of the corresponding device and the root bridge.
  – Number of the device port that leads to the root bridge.
  – Path cost from the root port of the device to the root bridge.

11 References

This chapter contains descriptions of the individual parameters that you configure via the graphical user interface.

Note: The content of the online help corresponds to the information in the “References” chapter of this configuration user manual.
Use the “Help” button to call up the online help in the graphical user interface.

11.1 Basic Settings

With this menu you can configure the basic settings of the device.

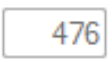
11.1.1 Basic Settings > System

This dialog displays the device properties.

System data

Parameter	Meaning
Name	Specifies the device name. Possible values: ▶ Alphanumeric ASCII character string with 0 to 255 characters
Location	Specifies the location of the device. Possible values: ▶ Alphanumeric ASCII character string with 0 to 255 characters
Contact	Specifies the contact person for this device. Possible values: ▶ Alphanumeric ASCII character string with 0 to 255 characters
Device Type	Displays the product name of the device.
Uptime	Displays the time that has elapsed since this device was last restarted. Possible values: ▶ Time in the format `day(s), hh:mm:ss`

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reload	Reloads the display of the page in your Web browser.
Set	Transfers the changes to the volatile memory of the device. To save the changes in the non-volatile local memory, proceed as follows: ☐ Open the `Basic Settings > Load/Save` dialog. ☐ Click "Save" in the "Load/Save" frame beside "Save current configuration".
Help	Opens the online help.

11.1.2 Basic Settings > Network

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

Management interface

Parameter	Meaning
IP address assignment	Specifies the source from which the device receives its IP parameters after starting: Possible values: ▶ `BOOTP` The device receives its IP parameters from a BOOTP or DHCP server. The server evaluates the MAC address of the device, then assigns the IP parameters. ▶ `DHCP` (state on delivery) The device receives its IP parameters from a DHCP server. The server evaluates the MAC address, the DHCP name, or other parameters of the device, then assigns the IP parameters. ▶ `Local` The device uses the IP parameters from the internal memory. You define the settings for this in the "IP Parameter" frame. **Note:** If there is no response from the BOOTP or DHCP server, the device sets the IP address to `0.0.0.0` and makes another attempt to obtain a valid IP address.
VLAN ID	Specifies the VLAN in which the device management is accessible through the network. The device management is accessible through ports that are members of this VLAN. Possible values: ▶ `1..4042` (default setting: `1`) The prerequisite is that the VLAN is already configured. See the Switching > VLAN > Configuration dialog. Assign a VLAN ID that is not assigned to any router interface. When you click the “Set“ 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 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 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 management VLAN.
MAC Address	Displays the MAC address of the device. The device management can be accessed via the network using the MAC address.

IP Parameters

Parameter	Meaning
IP Address	Specifies the IP address under which the device management can be accessed through the network. Possible values: ▶ Valid IPv4 address (default setting: —)
Netmask	Specifies the netmask. The netmask identifies the network prefix and the host address of the device in the IP address. Possible values: ▶ Valid IPv4 netmask (default setting: —)
Gateway address	Specifies the IP address of a router through which the device accesses other devices outside its own network. Possible values: ▶ Valid IPv4 address (default setting: —)

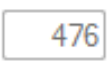
HiDiscovery protocol

On a PC the HiDiscovery software shows you the Hirschmann devices that can be accessed in the network on which the HiDiscovery function is activated. You can access these devices even if they have invalid IP parameters or none at all. The HiDiscovery software allows you to change the IP parameters in the device.

Parameter	Meaning
Operation	Activated/deactivates the HiDiscovery function in the device. Possible values: ▶ `On` (default setting) HiDiscovery is activated. You can access the device with the HiDiscovery software from your PC. ▶ `Off` HiDiscovery is deactivated.

Parameter	Meaning
Write Permission	Activates/deactivates the write access to the device using HiDiscovery. Possible values: ▶ `On` (default setting) The HiDiscovery software is given write access to the device. With this setting you can change the IP parameters in the device. ▶ `Off` The HiDiscovery software is only given read access to the device. With this setting you can view the IP parameters in the device. Recommendation: Change the setting to `Off` exclusively after putting the device into operation.

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reload	Reloads the display of the page in your Web browser.
Set	Transfers the changes to the volatile memory of the device. To save the changes in the non-volatile local memory, proceed as follows: ☐ Open the `Basic Settings > Load/Save` dialog. ☐ Click "Save" in the "Load/Save" frame beside "Save current configuration".
Help	Opens the online help.

11.1.3 Basic Settings > Software

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

Version

Parameter	Meaning
Bootcode	Displays the version number and creation date of the boot code.
Running Version	Displays the version number and creation date of the device software that the device loaded during the last restart and is currently running.

Software update

Parameter	Meaning
File	Specifies the path and the file name of the file with which you update the device software. The device allows you to update the device software via a TFTP download. ☐ Enter the URL for the file in the following format: `tftp://<IP address>/<path>/<file name>`
Upload	The device allows you to use Drag & Drop to save the file with which you are updating the device software. This option support the common Web browsers except the Internet Explorer. ☐ Use Drag & Drop to pull the file to the dotted area.
Install	Updates the device software The device installs the file specified in the "File" field, or saved using Drag & Drop, in the local non-volatile memory, replacing the previously saved device software. Upon restart, the device loads the installed device software.

Status

Parameter	Meaning
URL	Shows the URL for the file with which you are updating the device software.

Parameter	Meaning
Progress	Shows the progress of the device software update.

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
476	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reload	Reloads the display of the page in your Web browser.
Restart	Restarts the device.
Help	Opens the online help.

11.1.4 Basic settings > Load/Save

This dialog allows you to save the configuration profile. When you click “Set“ in a dialog while the device is operating, the device saves the changes temporarily solely.

You have the option of exporting configuration profiles to or copying them to the device.

Load/Save

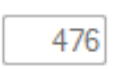
Parameter	Meaning
Save	Transfers the settings from the volatile memory (RAM) into the configuration profile in the non-volatile memory (NVM).

Parameter	Meaning
Reset	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`).

Configuration Transfer

Parameter	Meaning
Transfer Direction	Defines the transfer direction in which the configuration profile is transferred. Possible values: ▶ `Device to server` Select this value if you are transferring the configuration profile from the device. ▶ `Server to device` Select this value if you are transferring the configuration profile to the device.
Server IP address	Defines the IP address and the access path of the server from or to which the configuration profile is transferred. Enter the URL for the file in the following format: `tftp://<IP address>/<path>/<file name>`
Transfer	Transfers the configuration profile in the selected transfer direction.
Download	Exports the current configuration profile as a file in binary format.

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reload	Reloads the display of the page in your Web browser.
Help	Opens the online help.

11.1.5 Basic Settings > Port > Configuration

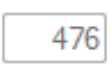
This dialog allows you to specify settings for the individual device ports. The dialog also displays the operating mode and connection status for every device port.

Configuration

Parameter	Meaning
Port	Displays the number of the device port.
State	Activates/deactivates the device port. Possible values: ▶ `On` (default setting) The device port is activated. ▶ `Off` The device port is deactivated. The device port does not send or receive any data.
Link/current operating mode	Displays the operating mode which the device port currently uses. Possible values: ▶ `-` No cable connected, no link ▶ `10 Mbit/s HDX` Half duplex connection ▶ `10 Mbit/s FDX` Full duplex connection ▶ `100 Mbit/s HDX` Half duplex connection ▶ `100 Mbit/s FDX` Full duplex connection

Parameter	Meaning
Manual configuration	Specifies the operating mode of the device port. Possible values: ▶ `Autoneg` (default setting) The device port negotiates the operating mode independently using autonegotiation and detects the devices connected to the TP port automatically (Auto Cable Crossing). This setting has priority over the manual setting of the device port. Elapse several seconds until the device port has set the operating mode. ▶ `10 Mbit/s HDX` Half duplex connection ▶ `10 Mbit/s FDX` Full duplex connection ▶ `100 Mbit/s HDX` Half duplex connection ▶ `100 Mbit/s FDX` (default setting on TP ports) Full duplex connection
Link monitoring	Activates/deactivates the reporting of detected link errors. Possible values: ▶ `On` The link monitoring is activated. ▶ `Off` The link monitoring is deactivated.

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reload	Reloads the display of the page in your Web browser.
Set	Transfers the changes to the volatile memory of the device. To save the changes in the non-volatile local memory, proceed as follows: ☐ Open the `Basic Settings > Load/Save` dialog. ☐ Click "Save" in the "Load/Save" frame beside "Save current configuration".
Help	Opens the online help.

11.1.6 Basic Settings > Port > Statistics

This frame displays the following overview per device port:

- Number of data packets/bytes sent from the device
  - "Transmitted Packets"
  - "Sent Unicast Packets"
  - "Sent Non Unicast Packets"

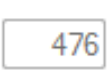
- Number of data packets/bytes received on the device
  - "Received Packets"
  - "Received Bytes"

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

- Number of data packets per size category received on and sent from the device
  - "Packets 64 byte"
  - "Packets 65 to 127 byte"
  - "Packets 128 to 255 byte"
  - "Packets 256 to 511 byte"
  - "Packets 512 to 1023 byte"
  - "Packets 1024 to 1518 byte"

To reset the counter for the port statistics in the table to `0`, click the “Reset port counters“ button in the `Basic Settings > Port > Statistics` dialog.

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reset the port counter	Resets the port statistic entries in the table to `0`.

Help	Opens the online help.

11.2 Device Security

This menu allows you to specify the settings for the access to the device.

11.2.1 Device Security > Password

The device allows users to access its management functions when they log in with valid login data.

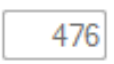
Selecting a password (HTTPS/SNMPv3)

Parameter	Meaning
Select Password	Displays the password to be changed. Possible values: ▶ `Modify read-only Password (user)` Changes the password for read access ▶ `Modify read\write Password (admin)` Changes the password for read and write access.
Current Administrator Password	Here you enter the administrator password.
New Password	Here you enter the new password. The minimum password length is 8 characters. Possible values: ▶ a-z, A-Z ▶ #$%&#()*+,-./:;<=>?@[]^_‘{}~!|
Please retype	Here you enter the new password again.

Activate user account (read-only)

Parameter	Meaning
Current Administrator Password	Here you enter the administrator password.
Activate user (user)	Activates the user account. When you activate the user account, a user can access the device with the `user/public` credentials.

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reload	Reloads the display of the page in your Web browser.
Set	Transfers the changes to the volatile memory of the device. To save the changes in the non-volatile local memory, proceed as follows: ☐ Open the `Basic Settings > Load/Save` dialog. ☐ Click "Save" in the "Load/Save" frame beside "Save current configuration".
Help	Opens the online help.

11.2.2 Device Security > HTTPS

This dialog allows you to specify settings for the HTTPS server of the device and to restart the server.

The HTTP server provides the graphical user interface (GUI) via an encrypted HTTP connection. The graphical user interface communicates with the device based on SNMP via the encrypted HTTP connection and enables access to the management functions.

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

Configuration

Parameter	Meaning
Web Interface Session Timeout [s]	Specifies the timeout in seconds. After the device has been inactive for this time it ends the session for the user logged on.
TCP Port	Specifies the number of the TCP port on which the server receives requests from clients. Possible values: ▶ `1..65535` (default setting: `443`) The server restarts automatically after the port is changed. In the process, the device terminates open connections to the server.

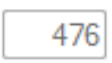
Certificate

Parameter	Meaning
Status	Displays whether the digital certificate is present on the device. Possible values: ▶ `Certificate present` The certificate is present. ▶ `No certificate present` The certificate has been removed. ▶ `Certificate will be created ...` The certificate is being created on the device. ▶ `Certificate created` The certificate has been created on the device.

Parameter	Meaning
Create	Creates a digital certificate on the device. To get the server to use this certificate, click the “Create“ button and restart the server using the "Restart Web server" button. Alternatively, you have the option of copying your own certificate to the device.
Delete	Deletes the digital certificate. To remove the certificate from the device, save the changes. In the process, the device switches off the HTTPS server.
File	Specifies the path and file name of the certificate. X.509 certificates (PEM) are permitted. The device gives you the following options for copying the certificate to the device: ▶ Import from the PC If the certificate is on your PC or on a network drive, select the file to be imported and use Drag & Drop to pull it into the dotted area. This option support the common Web browsers except the Internet Explorer. ▶ Import from a TFTP server If the certificate is on a TFTP server, enter the URL for the file in the following form: `tftp://<IP address>/<Path>/<File name>`
Upload	If the certificate is on your PC or on a network drive, select the file to be imported and use Drag & Drop to pull it into the dotted area.
Import	Copies the certificate to the device. To get the server to use this certificate, click the “Set“ button and restart the server.
Restart Web server	Restarts the HTTPS service of the device.

Note: In the Web browser, a message appears when you are loading the graphical user interface if you are using a certificate that has not been verified by a certifying organization. To load the graphical user interface, add an exception rule for the certificate in the Web browser.

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
	Displays the time in seconds after which the device automatically ends the session when the user is inactive.

Reload	Reloads the display of the page in your Web browser.
Set	Transfers the changes to the volatile memory of the device. To save the changes in the non-volatile local memory, proceed as follows: ☐ Open the `Basic Settings > Load/Save` dialog. ☐ Click "Save" in the "Load/Save" frame beside "Save current configuration".
Help	Opens the online help.

11.2.3 Device Security > SNMP

This dialog allows you to specify settings for the SNMP agent of the device and to enable/disable access to the device with different SNMP versions.

The SNMP agent activates access to the management functions of the device with SNMP-based applications, for example with the graphical user interface.

Configuration

Parameter	Meaning
SNMPv1 enabled	Activates/deactivates the access to the device with SNMP version 1. Possible values: ▶ `marked` (default setting) Access activated ▶ `unmarked` Access deactivated You define the community name in the `SNMPv1/v2 Community` frame.
SNMPv2 enabled	Activates/deactivates the access to the device with SNMP version 2. Possible values: ▶ `marked` (default setting) Access activated ▶ `unmarked` Access deactivated You define the community name in the `SNMPv1/v2 Community` frame.

Parameter	Meaning
SNMPv3 enabled	Activates/deactivates the access to the device with SNMP version 3. Possible values: ▶ `marked` (default setting) Access activated ▶ `unmarked` Access deactivated This function uses, for example, the Industrial HiVision software to make changes to the settings.
Port Number	Specifies the number of the UDP port on which the SNMP agent receives requests from clients. Possible values: ▶ `1..65535` (default setting: `161`) To enable the SNMP agent to use the new port after a change, you proceed as follows: ☐ Click the “Set“ button. ☐ In the `Basic Settings > Load/Save` dialog, click the “Save“ button beside "Save current configuration". ☐ Restart the device.

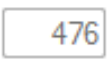
SNMPv1/v2 Community

This frame displays the authorization for SNMPv1/v2 applications to the device:

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

Parameter	Meaning
Read	Specifies the community name for the adjacent authorization. Possible values: ▶ Alphanumeric ASCII character string with 0 to 32 characters public (default setting for read authorization)
Write	Specifies the community name for the adjacent authorization. Possible values: ▶ Alphanumeric ASCII character string with 0 to 32 characters private (default setting for read and write authorization)

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reload	Reloads the display of the page in your Web browser.
Set	Transfers the changes to the volatile memory of the device. To save the changes in the non-volatile local memory, proceed as follows: ☐ Open the `Basic Settings > Load/Save` dialog. ☐ Click "Save" in the "Load/Save" frame beside "Save current configuration".
Help	Opens the online help.

11.3 Time

11.3.1 Time> Basic Settings

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

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

Parameter	Meaning
System Time (UTC)	Displays the current date and time with reference to Universal Time Coordinated (UTC).
System Time	Displays the current date and time with reference to the local time: “System Time“ = “System Time (UTC)“ + “Local Offset [min]“
Time Source	Displays the time source from which the device gets the time information. The device automatically selects the available time source with the greatest accuracy. Possible values: ▶ `local` System clock of the device. ▶ `sntp` The SNTP client is activated and the device is synchronized by an SNTP server.
Local Offset [min]	Defines the difference between the local time and “System Time (UTC)” in minutes: “Local Offset [min]” = “System Time” − “System Time (UTC)” Possible values: ▶ `-780..840` (default setting: `60`)
Set Time from PC	The device uses the time on the PC as the system time.

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
476	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reload	Reloads the display of the page in your Web browser.
Set	Transfers the changes to the volatile memory of the device. To save the changes in the non-volatile local memory, proceed as follows: ☐ Open the `Basic Settings > Load/Save` dialog. ☐ Click "Save" in the "Load/Save" frame beside "Save current configuration".
Help	Opens the online help.

11.3.2 Time> SNTP

The Simple Network Time Protocol (SNTP) is a procedure described in the RFC 4330 for time synchronization in the network. The device allows you to synchronize the system time in the device as an SNTP client.

Operation

Parameter	Meaning
Operation	Enables/disables the SNTP Client function of the device. Possible values: ▶ `On` The SNTP Client function is enabled. The device operates as an SNTP client. ▶ `Off` The SNTP Client function is disabled.

Configuration

Parameter	Meaning
Mode	Specifies whether the device actively requests the time information from an SNTP server known and configured in the network (Unicast mode) or passively waits for the time information from a random SNTP server (Broadcast mode). Possible values: ▶ `unicast` (default setting) The device takes the time information from the configured SNTP server exclusively. The device sends Unicast requests to the SNTP server and evaluates its responses. ▶ `broadcast` The device obtains the time information from one or more SNTP or NTP servers. The device evaluates the Broadcasts or Multicasts from these servers exclusively.
Request Interval [s]	Specifies the interval in seconds at which the device requests time information from the SNTP server. Possible values: ▶ `5..3600` (default setting: `30`)
Broadcast recv timeout [s]	Specifies the time in seconds a client in broadcast client mode waits before changing the value in the field from `syncToRemoteServer` to `notSynchronized` when the client receives no broadcast packets. Possible values: ▶ `128..2048` (default setting: `3`)
Disable client after successful sync	Activates/deactivates the disabling of the SNTP client after the device has successfully synchronized the time. Possible values: ▶ `marked` The disabling of the SNTP client is active. The device deactivates the SNTP client after successful time synchronization. ▶ `unmarked` (default setting) The disabling of the SNTP client is inactive. The SNTP client remains active after successful time synchronization.

Status

Parameter	Meaning
Status	Displays the status of the SNTP client. Possible values: ▶ `no server` The SNTP client is disabled. ▶ `notSynchronized` The SNTP client is not synchronized with any SNTP or NTP server. ▶ `synchronizedToRemoteServer` The SNTP client is synchronized with an SNTP or NTP server.

Stratum

Parameter	Meaning
Stratum	Displays the.distance between a network device and an authoritative time source. Possible values: ▶ `0` Unspecified or invalid. ▶ `1` Primary server (e.g., equipped with a GPS receiver). ▶ `2..15` Secondary server (via NTP). ▶ `16` Unsynchronized. ▶ `17..255` Reserved.

Server time

Parameter	Meaning
Server time	Displays.the time value synchronized with the SNTP server. Possible values: ▶ Time in the format `DD.MM.YYYY HH:MM:SS UTC`

Table

Parameter	Meaning
Index	Displays the index number to which the table entry relates. Possible values: ▶ `1..2` The device automatically assigns this number. When you delete a table entry, this leaves a gap in the numbering. When you create a new table entry, the device fills the first gap. After starting, the device sends requests to the SNTP server configured in the first table entry. If the server does not reply, the device sends its requests to the SNTP server configured in the next table entry. If none of the configured SNTP servers responds in the meantime, the SNTP client loses its synchronization. The device cyclically sends requests to each SNTP server until a server delivers a valid time. The device synchronizes itself with this SNTP server, even if the other servers can be reached again later.
Name	Specifies the name of the SNTP server. Possible values: ▶ Alphanumeric ASCII character string with 1..32 characters
Address	Specifies the IP address of the SNTP server. Possible values: ▶ Valid IPv4 address (default setting: `0.0.0.0`)
Destination UDP port	Specifies the UDP Port on which the SNTP server expects the time information. Possible values: ▶ `1..65535` (default setting: `123`)

Parameter	Meaning
Status	Displays the connection status between the SNTP client and the SNTP server. Possible values: ▶ `success` The device has successfully synchronized the time with the SNTP server. ▶ `badDateEncoded` The time information received contains protocol errors - synchronization failed. ▶ `other` – The value `0.0.0.0` is entered for the IP address of the SNTP server - synchronization failed. or – The SNTP client is using a different SNTP server. ▶ `requestTimedOut` The device has not received a reply from the SNTP server - synchronization failed. ▶ `serverKissOfDeath` The SNTP server is overloaded. The device is requested to synchronize itself with another SNTP server. If no other SNTP server is available, the device asks at intervals longer than the setting in the Request interval [s] field, whether the server is still overloaded. ▶ `serverUnsychronized` The SNTP server is not synchronized with either a local or an externalreference clock - synchronization failed. ▶ `versionNotSupported` The SNTP versions on the client and the server are incompatible with each other - synchronization failed.
Active	Activates/deactivates the connection to the SNTP server. Possible values: ▶ `marked` The connection to the SNTP server is activated. The SNTP client has access to the SNTP server. ▶ `unmarked` (default setting) The connection to the SNTP server is deactivated. The SNTP client has no access to the SNTP server.

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.

476	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reload	Reloads the display of the page in your Web browser.
Set	Transfers the changes to the volatile memory of the device. To save the changes in the non-volatile local memory, proceed as follows: ☐ Open the `Basic Settings > Load/Save` dialog. ☐ Click "Save" in the "Load/Save" frame beside "Save current configuration".
Add server	Adds a new table entry.
Help	Opens the online help.

11.4 Switching

This menu allows you to specify the settings for the access to the device.

11.4.1 Switching > Global

According to standard IEEE 802.1Q, the device forwards data packets with a VLAN tag in a VLAN ≥ 1. However, a small number of applications on connected end devices send or receive data packets with a VLAN ID=0. When the device receives one of these data packets, before forwarding it the device overwrites the original value in the data packet with the VLAN ID of the receiving port. When you activate the “VLAN unaware mode“, this deactivates the VLAN settings in the device. The device then transparently forwards the data packets and evaluates the priority information contained in the data packet exclusively.

Parameter	Meaning
MAC address	Displays the MAC address of the device.
Aging time [s]	Specifies the aging time in seconds. Possible values: ▶ 10..500000 (default setting: 30) The device monitors the age of the learned unicast MAC addresses. The device deletes address entries that exceed a particular age (aging time) from its address table. You find the address table in the Switching > Filter for MAC Addresses dialog. In connection with the router redundancy, specify a time ≥ 30s.

Parameter	Meaning
VLAN unaware mode	Activates/deactivates the VLAN unaware mode. Possible values: ▶ `marked` The VLAN unaware mode is active. The device works in the VLAN Unaware bridging mode (802.1Q): – The device ignores the VLAN settings in the device and the VLAN tags in the data packets. The device transmits the data packets based on their destination MAC address or destination IP address in VLAN `1`. – The device ignores the VLAN settings specified in the Switching > VLAN > Configuration and Switching > VLAN > Port dialogs. Every port is assigned to VLAN 1. – The device evaluates the priority information contained in the data packet. **Note:** You specify the VLAN ID `1` for every function on the device which uses VLAN settings. Among other things, this applies to static filters, MRP and IGMP Snooping. ▶ `unmarked` (default setting) The VLAN unaware mode is inactive. The device works in the VLAN Aware bridging mode (802.1Q): – The device evaluates the VLAN tags in the data packets. – The device transmits the data packets based on their destination MAC address or destination IP address in the corresponding VLAN. – The device evaluates the priority information contained in the data packet.

11.4.2 Switching > Filter for MAC Addresses

This dialog allows you to display and edit address filters for the address table (forwarding database). Address filters specify the way the data packets are forwarded in the device based on the destination MAC address.

Each row in the table represents one filter. The device automatically sets up the filters. The device allows you to set up additional filters manually.

The device transmits the data packets as follows:

- If the table contains an entry for the destination address of a data packet, the device transmits the data packet from the receiving port to the port specified in the table entry.
- If there is no table entry for the destination address, the device transmits the data packet from the receiving port to every other port.

Table

Parameter	Meaning
Address	Displays the destination MAC address to which the table entry applies.
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. ▶ `static` Address filter set up manually. The address filter stays set up.
Port	Displays the device port to which the table entry is assigned.
Remove	Deletes the adjacent destination address from the MAC address table.

To remove the learned MAC addresses from the address table (forwarding database), click the “Reset MAC Address Table“ button.

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.

476	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reload	Reloads the display of the page in your Web browser.
Reset MAC Address Table	Removes the MAC addresses from the forwarding table that have the value `learned` in the “Status“ field.
Create	Opens the "Create Entry" dialog to add a new entry to the table. ▶ In the “Address“ field, you specify the destination MAC address. ▶ In the “Possible Ports“ field, you specify the device port. – Select one port if the destination MAC address is a unicast address. – Select one or more ports if the destination MAC address is a multicast address. – Select no port to create a discard filter. The device discards data packets with the destination MAC address specified in the table entry.
Help	Opens the online help.

11.4.3 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 a minimum bandwidth for specific applications. The prerequisite for this 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 (e.g. priority for management packets, port priority).

11.4.4 Switching > QoS/Priority > Port Configuration

In this dialog, you specify the QoS/priority settings for each device port for received data packets.

Table

Parameter	Meaning
Port	Displays the number of the device port.
Port Priority	Specifies the VLAN priority of the data packets that the port receives. The device applies this setting to data packets depending on the value in the "Trust Mode" column: – “Trust Mode“ =`untrusted` The device transmits the data packet with the VLAN priority specified here. – “Trust Mode“ = `trustDot1p` If the data packet does not contain any VLAN or priority tag, the device transmits the data packet with the VLAN priority specified here. – “Trust Mode“ = `trustIpDscp` If the data packet is not an IP packet, the device transmits the data packet with the priority specified here. 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. 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.

Parameter	Meaning
Trust mode	Specifies how the device handles received data packets that contain a QoS/priority information. Possible values: ▶ `untrusted` The device transmits the data packet with the VLAN priority specified in the “Port Priority“ field. The device ignores the QoS/priority information contained in the data packet. ▶ `trustDot1p` (default setting) – If the data packet contains a VLAN tag, the device transmits the data packet based on the contained QoS/priority information. In the `Switching > QoS/Priority > 802.1D/p Mapping` dialog, you assign a traffic class to every VLAN priority. 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. – If the data packet does not contain a VLAN tag, the device transmits the data packet with the VLAN priority specified in the “Port Priority“ field. ▶ `trustIpDscp` – If the data packet is an IP data packet, the device transmits the data packet based on the contained IP DSCP value. In the `Switching > QoS/Priority > IP DSCP Mapping` dialog you assign a traffic class to every IP DSCP value. 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. – If the data packet is not an IP data packet, the device transmits the data packet with the VLAN priority specified in the “Port Priority“ field.
Untrusted traffic class	Displays the traffic class. The device assigns data packets to this traffic class if in the “Trust Mode“ field the value `untrusted` is specified. Possible values: ▶ `0..3` In the `Switching > QoS/Priority > 802.1D/p Mapping` dialog, you assign a traffic class to every VLAN priority. 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.

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
	Displays the time in seconds after which the device automatically ends the session when the user is inactive.

Reload	Reloads the display of the page in your Web browser.
Set	Transfers the changes to the volatile memory of the device. To save the changes in the non-volatile local memory, proceed as follows: ☐ Open the `Basic Settings > Load/Save` dialog. ☐ Click "Save" in the "Load/Save" frame beside "Save current configuration".
Help	Opens the online help.

11.4.5 Switching > QoS/Priority > 802.1D/p Mapping

The device transmits data packets with a VLAN tag according to the contained QoS/priority information with a higher or lower priority.

In this dialog, you assign a traffic class to every VLAN priority. You assign the traffic classes to the priority queues of the ports.

Table

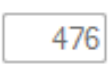
Parameter	Meaning
VLAN Priority	Displays the VLAN priority.
Traffic class	Specifies the traffic class assigned to the VLAN priority. Possible values: ▶ `0` assigned to the priority queue with the lowest priority. **Note:** Network management protocols and redundancy mechanisms use the highest traffic 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`		Standard Normal Data

VLAN priority	Traffic Class	Content description according to IEEE 802.1D
1		Background Non-time critical data and background services
2		Background Non-time critical data and background services
3		Standard Normal Data
4		Best Effort Normal data without prioritizing
5		Best Effort Normal data without prioritizing
6		Excellent Effort Important data
7		Excellent Effort Important data

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reload	Reloads the display of the page in your Web browser.
Set	Transfers the changes to the volatile memory of the device. To save the changes in the non-volatile local memory, proceed as follows: ☐ Open the `Basic Settings > Load/Save` dialog. ☐ Click "Save" in the "Load/Save" frame beside "Save current configuration".
Help	Opens the online help.

11.4.6 QoS/Priority > IP DSCP Mapping

The device transmits IP data packets according to the DSCP value contained in the data packet with a higher or lower priority.

In this dialog, you assign a traffic class to every DSCP value. You assign the traffic classes to the priority queues of the ports.

Table

Parameter	Meaning
DSCP Value	Displays the DSCP value.
Traffic class	Specifies the traffic class assigned to the DSCP value. Possible values: ▶ `0` assigned to the priority queue with the lowest priority.

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
476	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reload	Reloads the display of the page in your Web browser.
Set	Transfers the changes to the volatile memory of the device. To save the changes in the non-volatile local memory, proceed as follows: ☐ Open the `Basic Settings > Load/Save` dialog. ☐ Click "Save" in the "Load/Save" frame beside "Save current configuration".
Help	Opens the online help.

Default assignment of the DSCP values to traffic classes

DSCP Value	Traffic Class
`0-7`	

DSCP Value	Traffic Class
8-15	0
16-23	
24-31	
32-39	
40-47	
48-55	
56-63	

11.4.7 Switching> VLAN

With VLAN (Virtual Local Area Network) you distribute the data traffic in the physical network topological subnetworks. This provides you with the following advantages:

- High flexibility
  - With VLAN you distribute the data traffic to logical networks in the existing infrastructure.
    Without VLAN, it would be necessary to have additional devices and complicated cabling.
  - With VLAN you specify network segments independently of the location of the individual end devices.
- Improved throughput
  - In VLANs data packets can be transferred by priority.
    When the priority is high, the device transfers the data of a VLAN preferentially, for example for time-sensitive applications such as VoIP phone calls.
  - When the data packets and Broadcasts are distributed in small network segments instead of in the entire network, the network load is considerably reduced.
- Increased security
  The distribution of the data traffic among individual logical networks makes unwanted accessing more difficult and strengthens the system against attacks such as MAC Flooding or MAC Spoofing.

The device supports packet-based “tagged” VLANs according to the IEEE 802.1Q standard. The VLAN tagging in the data packet indicates the VLAN to which the data packet belongs.

The device transmits the tagged data packets of a VLAN only on ports that are assigned to the same VLAN. This reduces the network load.

The device prioritizes the received data stream in the following sequence:
- Voice VLAN
- MAC-based VLAN
- IP subnet-based VLAN
- Protocol-based VLAN
- Port-based VLAN

11.4.8 Switching> VLAN> Configuration

VLAN Global

This dialog allows you to view general VLAN parameters for the device.

Parameter	Meaning
Max. VLAN ID	Highest ID assignable to a VLAN. See the `Switching > VLAN > Configuration` dialog.
VLAN (max.)	Displays the maximum number of VLANs possible. See the `Switching > VLAN > Configuration` dialog.
VLANs	Number of VLANs currently configured in the device. See the `Switching > VLAN > Configuration` dialog. The VLAN ID 1 is always present in the device.

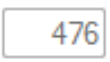
VLAN Configuration

In this dialog, you manage the VLANs. To set up a VLAN, create a further row in the table. There you specify for each port if it transmits data packets of the respective VLAN and if the data packets contain a VLAN tag.

Parameter	Meaning
VLAN ID	ID of the VLAN. The device supports up to 32 VLANs simultaneously. Possible values: ▶ `1..4042` (default setting: `1`)
Status	Displays how the VLAN is set up. Possible values: ▶ `other` VLAN 1 ▶ `permanent` VLAN set up by the user.
Creation time	Displays the time of VLAN creation. The field displays the time stamp for the operating time (system uptime).
Name	Specifies the name of the VLAN. Possible values: ▶ Alphanumeric ASCII character string with `1..32` characters
<Port number>	Specifies if the respective port transmits data packets of the VLAN and if the data packets containa 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. ▶ `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.

Note: Verify that the port on which the network management station is connected is a member of the VLAN in which the device transmits the management data. In the default setting, the device transmits the management data on VLAN 1. Otherwise, the connection to the device terminates when you transfer the changes to the device.

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Add	Adds a new table entry.
Reload	Reloads the display of the page in your Web browser.
Set	Transfers the changes to the volatile memory of the device. To save the changes in the non-volatile local memory, proceed as follows: ☐ Open the `Basic Settings > Load/Save` dialog. ☐ Click "Save" in the "Load/Save" frame beside "Save current configuration".
Help	Opens the online help.

11.4.9 Switching> VLAN> Port

In this dialog you specify how the device handles received data packets that have no VLAN tag, or whose VLAN tag differs from the VLAN ID of the port.

This dialog lets you assign a VLAN to the ports and thus specify the port VLAN ID.

Additionally, you also specify for each port how the device transmits data packets if the VLAN Unaware mode is disabled and one of the following situations occurs:

- The port receives data packets without a VLAN tagging.
- The port receives data packets with VLAN priority information (VLAN ID 0, priority tagged).
- The VLAN tagging of the data packet differs from the VLAN ID of the port.

Table

Parameter	Meaning
Port	Displays the port number.
Port VLAN ID	Specifies the ID of the VLAN which the devices assigns to data packets without a VLAN tag. The prerequisite is that you specify in the `Acceptable packet types` column the value `admitAll`. Possible values: ▶ ID of a VLAN you set up (default setting: `1`)
Acceptable packet types	Specifies whether 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. ▶ `admitTaggedOnly` The port accepts only data packets tagged with a VLAN ID ≥ `1`.
Ingress filtering	Activates/deactivates the ingress filtering. Possible values: ▶ `marked` The ingress filtering is active. The device compares the VLAN ID in the data packet with the VLANs of which the device is a member. See the `Switching > VLAN > Configuration` dialog. If the VLAN ID in the data packet matches one of these VLANs, then the port transmits the data packet. Otherwise, the device discards the data packet. ▶ `unmarked` (default setting) The ingress filtering is inactive. The device transmits received data packets without comparing the VLAN ID. Thus the port also transmits data packets with a VLAN ID of which the port is not a member.

11.4.10Switching > L2 Redundancy > MRP Client

The device supports MRP Client functionality according to IEC 62439.

You can configure the MRP client with the Graphical User Interface (GUI) or with Profinet IO.

The MRP client supports both, 200ms and 500ms reconfiguration times. To achieve the low reconfiguration times, the device implements fast Link-Detection and the device sends Link-Down Notifications on the ring-ports.

The MRP operation supports up to 100 Ring Nodes.

MRP-Client

Parameter	Meaning
Operation	Enables/disables the MRP Client function. After you configured the parameters for the MRP ring, enable the function here. Possible values: ▶ On The MRP-Client function is enabled. After you configured the devices in the MRP ring, the redundancy is active. ▶ Off (default setting) The MRP-Client function is disabled.

Ring port 1/Ring port 2

Parameter	Meaning
Port	Specifies the number of the port that is operating as a ring port. Possible values: ▶ <Port number> Number of the ring port
Operation	Displays the operating status of the ring port. Possible values: ▶ forwarding The port is enabled, connection exists. ▶ blocked The port is blocked, connection exists. ▶ disabled The port is disabled. ▶ not-connected No connection exists.

Configuration

Parameter	Meaning
Domain ID	Displays/Configures the Domain ID. (default setting: Default) (255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255)
Domain Name	Display/Configures the domain name. (default setting: empty string)
VLAN ID	Specifies the ID of the VLAN which you assign to the ring ports. Possible values: ▶ 0 (default setting) No VLAN assigned. Assign in the Switching > VLAN > Configuration dialog to the ring ports for VLAN 1the value U. ▶ 1..4042 VLAN assigned. If you assign to the ring ports a non-existing VLAN, the device creates this VLAN. In the Switching > VLAN > Configuration dialog, the device creates an entry in the table for the VLAN and assigns the value T to the ring ports.

Information

Parameter	Meaning
Information	Displays messages for the redundancy configuration and the possible causes of errors. The following messages are possible if the device operates as a ring client: ▶ `Redundancy available` The redundancy is set up. When a component of the ring is down, the redundant line takes over its function. ▶ `Configuration error: Error on the ring port link.` Error in the cabling of the ring ports.

11.4.11 Switching > L2 Redundancy > Spanning Tree > Global

This dialog allows you to configure and monitor the settings for redundancy procedure.

The device supports the Rapid Spanning Tree Protocol (RSTP) defined in standard IEEE 802.1D-2004. This protocol is a further development of the Spanning Tree Protocol (STP) and is compatible with it.

The Spanning Tree Protocol (STP) is a protocol that deactivates redundant paths of a network in order to help avoid loops. If a network component is unsuccessful on the path, the device calculates the new topology and reactivates these paths.

The Rapid Spanning Tree Protocol enables fast switching to a newly calculated topology without interrupting existing connections.

Spanning tree

Parameter	Meaning
Operation	Enables/disables the Spanning Tree function in the device. Possible values: ▶ `On` (Default setting) ▶ `Off` The device behaves transparently. The device floods received Spanning Tree data packets like multicast data packets to the device ports.

Protocol Configuration/Information

“Bridge“

Parameter	Meaning
Bridge ID	Displays the bridge ID of the device. The device with the numerically lowest bridge ID takes over the role of the root bridge in the network. Possible values: ▶ `<Bridge priority> / <MAC address>`

Parameter	Meaning
Priority	Specifies the bridge priority of the device. Possible values: ▶ `0..61440` in steps of 4096 (default setting: `32,768`) Assign the lowest numeric priority in the network to the device to make it the root bridge.
Hello Time [s]	Specifies the time in seconds between the sending of two configuration messages (Hello data packets). Possible values: ▶ `2` If the device takes over the role of the root bridge, the other devices in the network use the value specified here. Otherwise, the device uses the value specified by the root bridge, see the “Root“ column.
Forward Delay [s]	Specifies the delay time for the status change in seconds. Possible values: ▶ `4..30` (default setting: `15`) If the device takes over the role of the root bridge, the other devices in the network use the value specified here. Otherwise, the device uses the value specified by the root bridge, see the “Root“ column. In the RSTP protocol, the bridges negotiate a status change without a specified delay. The STP protocol uses the parameter to delay the status change between the statuses `disabled`, `discarding`, `learning`, `forwarding`.
The parameters "Forward Delay" and "Max Age" have the following relationship: `Forward Delay` ≥ (`Max Age`/2) + 1 If you enter values in the fields that contradict this relationship, the device replaces these values with the last valid values or with the default value.	
Max Age	Specifies the maximum permissible branch length, for example the number of devices to the root bridge. Possible values: ▶ `6..40` (default setting: `20`) If the device takes over the role of the root bridge, the other devices in the network use the value specified here. Otherwise, the device uses the value specified by the root bridge, see the “Root“ column. The STP protocol uses the parameter to specify the validity of STP-BPDUs in seconds.

“Root“

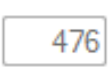
Parameter	Meaning
Bridge ID	Displays the bridge ID of the current root bridge. Possible values: ▶ `<Bridge priority> / <MAC address>` The bridge ID is made up of the bridge priority and the MAC address.
Priority	Displays the bridge priority of the current root bridge. Possible values: ▶ `0..61440` in steps of 4096
Hello Time [s]	Displays the time in seconds specified by the root bridge between the sending of two configuration messages (Hello data packets). Possible values: ▶ `1..2` The device uses this specified value - see the "Bridge" column.
Forward Delay [s]	Displays the delay time in seconds set up by the root bridge for status changes. Possible values: ▶ `4..30` The device uses this specified value, see the “Bridge“ column. In the RSTP protocol, the bridges negotiate a status change without a specified delay. The STP protocol uses the parameter to delay the status change between the statuses `disabled`, `discarding`, `learning`, `forwarding`.
Max Age	Displays the maximum permissible branch length set up by the root bridge, for example the number of devices to the root bridge. Possible values: ▶ `6..40` (default setting: `20`) The STP protocol uses the parameter to specify the validity of STP-BPDUs in seconds.

“Topology“

Parameter	Meaning
Bridge is Root	Displays whether the device currently has the role of the root bridge. Possible values: ▶ `unmarked` Another device currently has the role of the root bridge. ▶ `marked` The device currently has the role of the root bridge.

Parameter	Meaning
Root Port	Displays the number of the device port from which the current path leads to the root bridge. If the device takes over the role of the root bridge, the field displays the value `0`.
Topology Change Count	Displays how often the device has put a device port into the `forwarding` status via Spanning Tree since it was started.
Time Since Topology Change	Displays the time since the last topology change. Possible values: ▶ <days, hours:minutes:seconds>
Root Path Cost	Specifies the path cost for the path that leads from the root port of the device to the root bridge of the layer 2 network. Possible values: ▶ `0..200000000` If the value `0` is specified, the device takes over the role of the root bridge.

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reload	Reloads the display of the page in your Web browser.
Set	Transfers the changes to the volatile memory of the device. To save the changes in the non-volatile local memory, proceed as follows: ☐ Open the `Basic Settings > Load/Save` dialog. ☐ Click "Save" in the "Load/Save" frame beside "Save current configuration".
Help	Opens the online help.

11.4.12 Switching > L2 Redundancy > Spanning Tree > Port

With this dialog you can switch the Spanning Tree function on/off on the device ports, specify edge ports, and specify the settings for various protection functions.

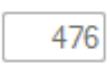
Table

Parameter	Meaning
Port	Displays the number of the device port.
Stp	Activates/deactivates the Spanning Tree function on the device port. Possible values: ▶ `On` (default setting) ▶ `Off` If the Spanning Tree is active in the device and inactive on the device port, the port does not send STP-BPDUs and drops any STP-BPDUs received.
Port priority	Specifies the priority of the device port. Possible values: ▶ `16..240` in steps of 16 (default setting: `128`) This value represents the first 4 bits of the port ID.
Port Path Cost	Specifies the RSTP port path cost to favor redundant paths (corresponds to a contribution of this port to the global root path cost). Possible values: Possible values: ▶ `0..200000000` (default setting: `200000`) If the value `0` is specified, the device automatically detects the path cost depending on the data rate.
Port Status	Displays the transmission status of the device port. Possible values: ▶ `discarding` The device port is blocked and forwards STP-BPDUs exclusively. ▶ `learning` The device port is blocked, but it learns the MAC addresses of received data packets. ▶ `forwarding` The device port forwards data packets. ▶ `disabled` The Spanning Tree function is inactive on the device port. The device port forwards STP-BPDUs. ▶ `disconnected` No cable is connected.

Parameter	Meaning
Port Role	Displays the current role of the port in CIST. Possible values: ▶ `root` Port with the cheapest path to the root bridge. ▶ `alternate` Port with the alternative path to the root bridge (currently interrupted). ▶ `designated` Port for the side of the tree averted from the root bridge. ▶ `backup` Port receives STP-BPDUs from its own device. ▶ `master` Port with the cheapest path to the CIST. The port is the CIST root port of the CIST Regional Root. The port is unique in an MST region. ▶ `disabled` The port is inactive. See the `Basic Settings> Port` dialog, `Configuration` tab.
Oper Edge Port	Displays whether a terminal device or an STP bridge is connected to the device port. Possible values: ▶ `enable` An end device is connected to the device port. The device port does not receive any STP-BPDUs. ▶ `disable` An STP bridge is connected to the device port. The device port receives STP-BPDUs.
Admin Edge Port	Specifies whether an end device is connected to the device port. Possible values: ▶ `unmarked` (default setting) An STP bridge is connected to the device port. After the connection is set up, the device port changes to the `learning` status before changing to the `forwarding` status, if applicable. ▶ `marked` An end device is connected to the device port. – After the connection is set up, the device port changes to the `forwarding` status without changing to the `learning` status beforehand. – If the device port receives an STP-BPDU, the device deactivates the port if the BPDU Guard function is enabled in the `Switching > L2-Redundancy > Spanning Tree > Global` dialog.

Parameter	Meaning
Auto Edge Port	Activates/deactivates the automatic detection of whether you connect an end device to the port. This setting is effective if you unmark the checkbox in the “Admin Edge Port“ field. Possible values: ▶ `marked` (default setting) After the installation of the connection, and after 1.5 × “Hello Time [s]“, the device sets the port to the `forwarding` status (default setting 1.5 × 2 s) if the port has not received any STP-BPDUs during this time. ▶ `unmarked` After the installation of the connection, and after “Max Age“, the device sets the port to the `forwarding` status (default setting 20 s).

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reload	Reloads the display of the page in your Web browser.
Set	Transfers the changes to the volatile memory of the device. To save the changes in the non-volatile local memory, proceed as follows: ☐ Open the `Basic Settings > Load/Save` dialog. ☐ Click "Save" in the "Load/Save" frame beside "Save current configuration".
Help	Opens the online help.

11.5 Secure Remote Access

11.5.1 Secure Remote Access> SiteManager GECKO

The SiteManager GECKO is a Hirschmann client which supports Secure Remote Access. It helps to build up secure connections of up to 10 devices which are connected to the SiteManager GECKO.

The dialog allows you to do the following:

- Specify basic settings for the SiteManager GECKO.
- Control the connection status to the GateManager Server and display the software version of the client.
- Reset the SiteManager GECKO Client to the default settings.
- Save a log file on the PC.

Configuration

Description	Meaning
Operation	When the function is on, the device initiates a connection to the GateManager. Possible values: ▶ “On“ The SiteManager GECKO initiates a permanent connection to the GateManager using the specified values. ▶ “Off“ (default setting) No connection to the GateManager.
GateManager Server	Specifies the IPv4 address of the GateManager Server. Possible values: ▶ Valid IPv4 address If the specified IP address in the configured subnet is unreachable, use a webproxy or a gateway. The "Basic Settings" > "Network” dialog, “IP Parameter” frame, “Gateway Address” field allows you to specify the gateway. Alternatively, you specify the gateway using HiDiscovery or a DHCP server. The “Webproxy Address”, “Webproxy Account” and “Webproxy Password” fields allow you to specify the data for the webproxy.
GateManager Token	Specifies the domain token for connecting to the GateManager GECKO. Possible values: ▶ Alphanumeric ASCII character string
Name	Specifies the description for the entry. Enter a name to describe the SiteManager GECKO. Possible values: ▶ Alphanumeric ASCII character string
Webproxy Address	Specifies the IPv4 address for the webproxy. Possible values: ▶ `[blank]` No webproxy. ▶ Valid IPv4 address Use a gateway, if the webproxy and GECKO are located in different subnets.
Webproxy Account	Specifies the user name with which the user authenticates on the webproxy.
Webproxy Password	Specifies the password with which the user authenticates on the webproxy.

Table 8: Configuration

Status

Description	Meaning
Status	Displays the connection status between the SiteManager GECKO and the GateManager. Possible values: ▶ `Starting` The device initiates the connection. The SiteManager GECKO verifies the validity of the GateManager's IP address. ▶ `Not connected` Connection between SiteManager GECKO and GateManager inactive. ▶ `Conncting to a.b.c.d` The device tries to establish the connection from the SiteManager GECKO to the GateManager. If you are using a webproxy, the device tries to establish the connection to the GateManager using the webproxy. ▶ `Connected to a.b.c.d` Connection between SiteManager GECKO and GateManager active.

Table 9: Status

SiteManager GECKO

Description	Meaning
Running Version	Displays the version number of the SiteManager GECKO that the device is currently running. The GateManager allows you to update the SiteManager GECKO only. The "Software Update" frame in the "Basic Settings" > "Software" dialog allows you to update the GECKO device software and the SiteManager simultaneously. See "Updating the software" on page 37

Table 10: SiteManager GECKO

Buttons

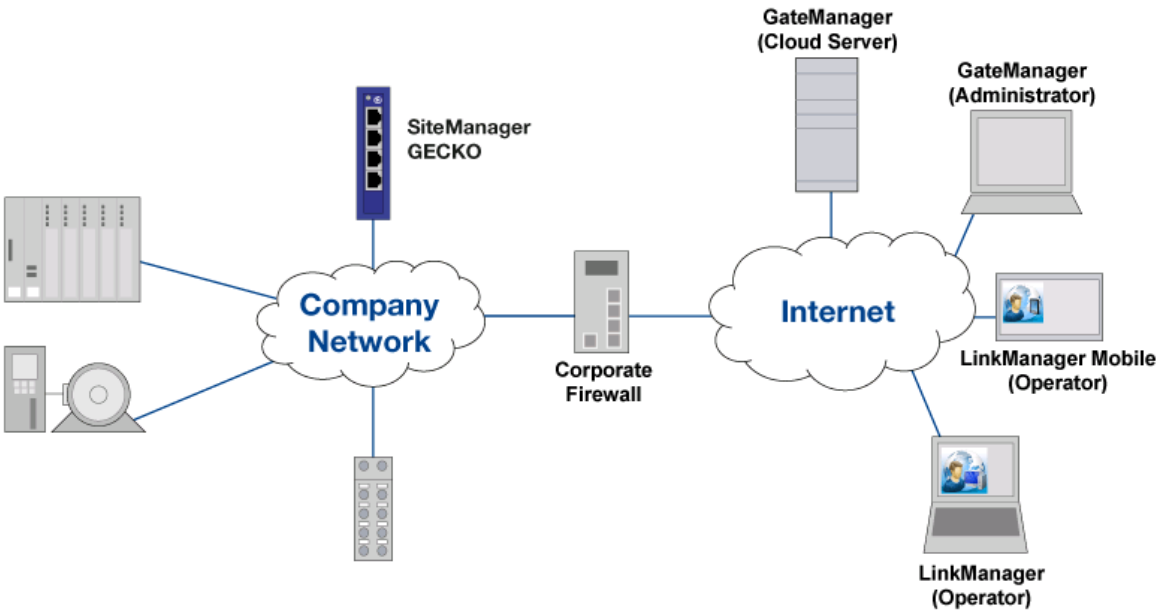
Reset	Reset SiteManager GECKO to factory default Resets the SiteManager GECKO to factory default. The device overwrites the updates which you have installed using the GateManager. The GECKO device software remains unmodified. You reset the complete GECKO device software, using the "Reset" button next to "Back to factory defaults" located in the "Basic Settings > Load/Save" dialog in the "Load/Save" frame.
Save	SiteManager GECKO Log Saves the "sitemanager_syslog0.txt" log file on your PC. The file contains detailed information about connections and run-time status.
Reload	Updates the fields with the values that are saved in the volatile memory(RAM) of the device.
Set	Transfers the changes to the volatile memory (RAM) of the device andapplies them to the device. To save the changes in the non-volatilememory, proceed as follows: ☐ Open`Basic Settings > Load/Save` dialog. ☐ Click the "Save" button in the "Load/Save" frame next to "Save current configuration".
Help	Opens the online help.

11.5.2 Secure Remote Access> About

In combination with the SiteManager GECKO, the device offers you a tool which assists you with a Secure Remote Access.

Secure Remote Access allows you to do the following:

- Connect devices which are located geographically away from each other.
- Remote programming of industrial components using familiar tools.
- Remote control and remote monitoring of industrial plants using your PC, iPhone or Android device.
- Operating machines without physical access to the network in which the machine is located.
- Applying secure mechanisms on devices which usually are classified as unsecure (tablets or smartphones).
- Creating accounts for machine operators with separate accounts to specific devices.


GateManager
(Cloud Server)
GateManager
(Administrator)
SiteManager
GECKO
Company
Network
Corporate
Firewall
Internet
LinkManager Mobile
(Operator)
LinkManager
(Operator)

11.6 Diagnostics

The dialogs in this menu show information on statuses and events that the device has logged. In service cases, this information helps our support to diagnose the situation.

11.6.1 Diagnosis >Alarms (Traps)

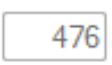
Alarms (Traps)

Parameter	Meaning
Operation	Specifies whether the device sends an SNMP trap when it detects a change in the monitored functions. Possible values: ▶ `On` The device sends an SNMP trap. ▶ `Off` (default setting) The device does not send an SNMP trap. The prerequisite for sending SNMP traps is that you enable the link monitoring in the `Basic settings > Port > Configuration` dialog and specify at least 1 SNMP manager (destination address).
Link Up/Down	At one port of the device, the link to a device connected there has been established/interrupted.
Authentication	The device has rejected an unauthorized access attempt. See “Device Security > SNMP” on page 88.
Spanning tree	The topology of the Rapid Spanning Tree has changed.
LLDP	Is sent if an entry in the topology discovery table is changed

Destination Addresses

Parameter	Meaning
IP Address	Specifies the IP address of the SNMP manager. Possible values: ▶ `Valid IPv4 address`
Trap Community	Specifies the name of the trap community that the device uses to identify itself as the source of the trap. Possible values: ▶ `public` (default setting) ▶ Alphanumeric ASCII character string with 0 to 64 characters

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reload	Reloads the display of the page in your Web browser.
Set	Transfers the changes to the volatile memory of the device. To save the changes in the non-volatile local memory, proceed as follows: ☐ Open the `Basic Settings > Load/Save` dialog. ☐ Click "Save" in the "Load/Save" frame beside "Save current configuration".
Help	Opens the online help.

11.6.2 Diagnosis > LLDP

The device allows you to gather information about neighboring devices. For this, the device uses the Link Layer Discovery Protocol (LLDP). This information enables the network management station to map the structure of your network.

Devices in networks send messages in the form of packets that are also known by the name “LLDPDU” (LLDP data unit). The data sent and received via LLDPDUs is useful for many reasons. For example, it enables the device to recognize which devices within the network are neighbors and via which ports they are connected with each other.

This dialog allows you to visualize the network and determine the connected devices and their function characteristics.

LLDP

Parameter	Meaning
Operation	If the function is switched on, the topology discovery with LLDP is activated on the device. Possible values: ▶ `On` (default setting) ▶ `Off`

Topology discovery

This dialog displays the collected LLDP information for the neighboring devices. This information enables the network management station to map the structure of your network.

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

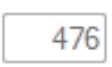
When only devices without active topology discovery are connected to a device port, the table will contain one line for this port to represent the devices. This line contains the number of connected devices.

The FDB address table contains MAC addresses of devices that the topology table hides for the sake of clarity.

If you use a port to connect several devices, for example via a hub, the table contains a line for each connected device.

Parameter	Meaning
Port	Displays the number of the device port.
Neighbor Identifier	Displays the chassis ID of the neighboring device. This can be the basis MAC address of the neighboring device, for example.
Neighbor IP Address	Displays the IP address with which the management functions of the neighboring device can be reached.
Neighbor Port Description	Displays a description for the device 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.

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reload	Reloads the display of the page in your Web browser.

Set	Transfers the changes to the volatile memory of the device. To save the changes in the non-volatile local memory, proceed as follows: ☐ Open the `Basic Settings > Load/Save` dialog. ☐ Click "Save" in the "Load/Save" frame beside "Save current configuration".
Help	Opens the online help.

11.6.3 Diagnosis > System Log

System Information

This dialog displays the current operating condition of individual components in the device.

The dialog allows you to save the page in HTML format on your PC.

System Log

The device logs specific device-internal events in a log file (system log).

This dialog displays the log file (system log). The dialog allows you to save the log file in HTML format on your PC.

The log file is kept until a restart is performed on the device. After the restart the device creates the file again.
To delete the logged events from the log file, click "Delete Log File".

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.

476	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reload	Reloads the display of the page in your Web browser.
Save	Opens the "Save" dialog. The dialog allows you to save the log file in HTML format on your PC.
Delete Log File	Removes the logged events from the log file.
Help	Opens the online help.

11.6.4 Diagnosis > Syslog

The device allows you to 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 2 syslog servers.

Syslog

Parameter	Meaning
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

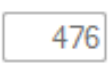
Parameter	Meaning
Index	Displays the index number to which the table entry relates. When you delete a table entry, this leaves a gap in the numbering. When you create a new table entry, the device fills the first gap. Possible values: ▶ 1..2
IP Address	Specifies the IP address of the syslog server. Possible values: ▶ Valid IPv4 address (default setting: 0.0.0.0)
Destination UDP Port	Specifies the TCP or UDP port on which the syslog server expects the log entries. Possible values: ▶ 1..65535 (default setting: 514)
Transport type	Displays the transport type the device uses to send the events to the syslog server.
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	Displays the type of the log entry transmitted by the device.
Active	Activates/deactivates the transmission of events to the syslog server: ▶ `marked` The device sends events to the syslog server. ▶ `unmarked` (default setting) The transmission of events to the syslog server is deactivated.

11.6.5 Diagnosis > Ports > SFP

This dialog allows you to look at the SFP transceivers currently connected to the device and their properties.
When the device is equipped with SFP transceivers, the table displays valid values.

Parameter	Meaning
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 whether the device supports the SFP transceiver.
Temperature [°C]	Temperature [°C] Operating temperature of the SFP transceiver in “Celsius.”
Tx power [mW]	Transmission power of the SFP transceiver in mW.
Rx power [mW]	Receiving power of the SFP transceiver in mW.
Tx power [dBm]	Transmission power of the SFP transceiver in dBm.
Rx power [dBm]	Receiving power of the SFP transceiver in dBm.

Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reload	Reloads the display of the page in your Web browser.
Help	Opens the online help.

11.7 Advanced

11.7.1 Advanced> Industrial Protocols> PROFINET

This dialog allows you to configure the PROFINET protocol on this device used in conjunction with PROFINET Controllers and PROFINET devices. The device bases the PROFINET function on the Siemens V2.2 PROFINET stack for common Ethernet controllers. The PROFINET protocol implemented in the device conforms to Class B for real time responses according to IEC 61158.

The following functions directly affect the PROFINET function. Verify that the parameters are set as described in the following table:

Parameter	Meaning
PROFINET	`Advanced > Industrial Protocols > PROFINET` dialog
	PROFINET frame Operation=`On`
	Configuration frame Name of station = <empty>
Network	`Basic Settings > Network` dialog
	Management Interface frame IP Address Assignment radio button = `Local`
	IP Parameters frame IP Address = `0.0.0.0` Netmask = `0.0.0.0` Gateway Address = `0.0.0.0`
	HiDiscovery Protocol frame Write Permission = `Off`
VLAN	`Switching > Global` dialog
	Configuration frame VLAN Unaware Mode checkbox = `marked`

Parameter	Meaning
LLDP	`Diagnostics > LLDP > Configuration` dialog Configuration frame Transmit interval [s] = `5` Transmit delay [s] = `1`
DHCP	`Basic Settings > Network` dialog Management Interface frame DHCP radio button = `unmarked`

PROFINET

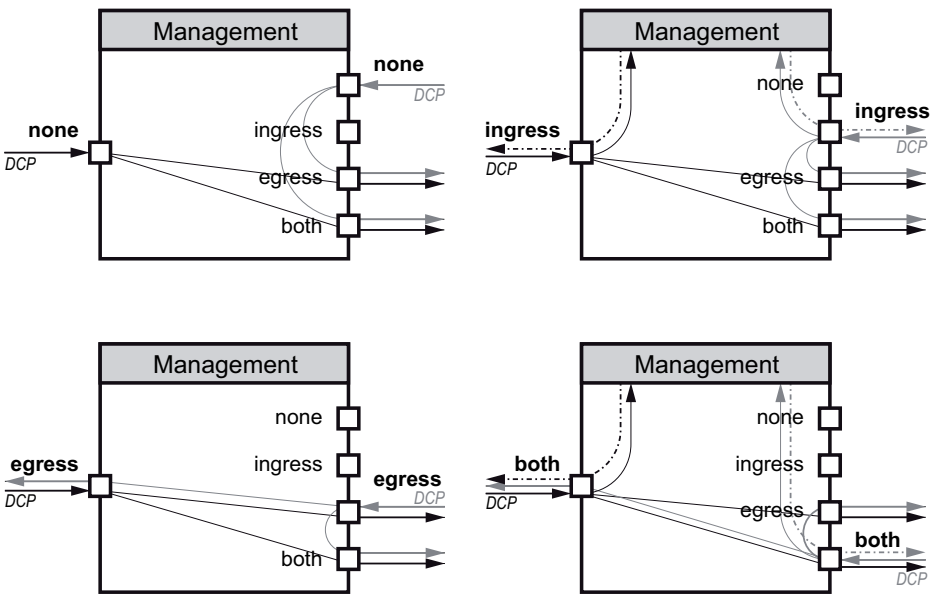
When you change the operational status of the function, a restart is required. To restart the device perform the following work steps:

☐ Open the `Basic Settings > Software` dialog.
☐ Click the “Restart“ button.

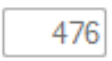
Parameter	Meaning
Operation	Enables/disables the PROFINET function on the device. Possible values: ▶ `On` The PROFINET function is enabled. **Note:** Verify that the Switching > Global > VLAN Unaware mode is enabled. ▶ `Off` (default setting) The PROFINET function is disabled.
Download GSDML file	Copies the GSDML file onto your PC.
AR Status	. Possible values: ▶ `Connected` . ▶ `Disconnected` (default setting) .

DCP Mode

When you activate the PROFINET function, the device displays the following values.

Parameter	Meaning
Port	Displays the port number.
DCP Mode	Specifies the data stream direction on the port to monitor for DCP packets. The Programmable Logic Controller (PLC) detects PROFINET devices using the Discovery and Configuration Protocol (DCP). The DCP identify request packets are multicast, the responses from the agents are unicast. Regardless of the settings, the device forwards the received DCP packets to other device ports whose setting is either `egress` or `both`.  Possible values: ▶ `none` The agent does not respond to packets received on this port. The port does not forward packets received on other ports. ▶ `ingress` The agent responds to packets received on this port. The port does not forward packets received on other ports. ▶ `egress` The agent does not respond to packets received on this port. The port forwards packets received on other ports. ▶ `both` (default setting) The agent responds to packets received on this port. The port forwards packets received on other ports.

11.7.2 Buttons

	Ends the session and terminates the connection to the device.
	Restarts the device.
	Displays the time in seconds after which the device automatically ends the session when the user is inactive.
Reload	Reloads the display of the page in your Web browser.
Set	Transfers the changes to the volatile memory of the device. To save the changes in the non-volatile local memory, proceed as follows: ☐ Open the `Basic Settings > Load/Save` dialog. ☐ Click "Save" in the "Load/Save" frame beside "Save current configuration".
Help	Opens the online help.

A Appendix

A.1 Technical Data

Switching	
Size of MAC address table (incl. static filters)	1,024
Max. number of statically configured MAC address filters	100
MTU (max. length of over-long packets)	1,522 bytes
Latency, depends on the port data rate 100 Mbit/s	min.7 µs max. 9 µs
Max. number of static address entries	100
Max. number of dynamic unicast entries	910
Number of priority queues	4 queues
Port priorities that can be set	0 ... 7

A.2 Underlying technical standards

ANSI/TIA-1057	Link Layer Discovery Protocol for Media Endpoint Devices, April 2006
IEEE 802.1AB	Topology Discovery (LLDP)
IEEE 802.1D-1998, IEEE 802.1 D-2004	Media access control (MAC) bridges (includes IEEE 802.1p Priority and Dynamic Multicast Filtering, GARP, GMRP)
IEEE 802.1Q-1998	Virtual Bridged Local Area Networks (VLAN Tagging, Port-Based VLANs, GVRP)
IEEE 802.1 Q-2005	Spanning Tree (STP), Rapid Spanning Tree (RSTP), Multiple Spanning Tree (MSTP)
IEEE 802.3-2002	Ethernet
IEEE 802.3x	Flow control

A.3 List of RFCs

RFC 768	UDP
RFC 783	TFTP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 951	BOOTP
RFC 1157	SNMPv1
RFC 1155	SMIv1
RFC 1212	Concise MIB Definitions
RFC 1213	MIB2
RFC 1493	Dot1d
RFC 1542	BOOTP Extensions
RFC 1643	Ethernet-like MIB
RFC 1757	RMON
RFC 1867	Form-based File Upload in HTML
RFC 1901	Community-based SNMP v2
RFC 1905	Protocol Operations for SNMP v2
RFC 1906	Transport Mappings for SNMP v2
RFC 1907	Management Information Base for SNMP v2
RFC 1908	Coexistence between SNMP v1 and SNMP v2
RFC 1945	HTTP/1.0
RFC 2068	HTTP/1.1
RFC 2131	DHCP
RFC 2132	DHCP Options
RFC 2233	The Interfaces Group MIB using SMI v2
RFC 2246	The TLS Protocol, Version 1.0
RFC 2271	SNMP Framework MIB
RFC 2346	AES Ciphersuites for Transport Layer Security
RFC 2365	Administratively Scoped Boundaries
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC 2475	An Architecture for Differentiated Service
RFC 2570	Introduction to SNMP v3
RFC 2571	Architecture for Describing SNMP Management Frameworks
RFC 2572	Message Processing and Dispatching for SNMP
RFC 2573	SNMP v3 Applications
RFC 2574	User Based Security Model for SNMP v3
RFC 2575	View Based Access Control Model for SNMP

RFC 2576	Coexistence between SNMP v1, v2 & v3
RFC 2578	SMIv2
RFC 2579	Textual Conventions for SMI v2
RFC 2580	Conformance Statements for SMI v2
RFC 2674	Dot1p/Q
RFC 2818	HTTP over TLS
RFC 2851	Internet Addresses MIB
RFC 4188	(Definitions of Managed Objects for Bridges)

A.4 Literature references

- “Optische Übertragungstechnik
  in industrieller Praxis”
  Christoph Wrobel (Hrsg.)
  Hüthig Buch Verlag Heidelberg
  ISBN 3-7785-2262-0

- „TCP/IP Illustrated“, Vol. 1
  W.R. Stevens
  Addison Wesley 1994
  ISBN 0-201-63346-9

- Hirschmann“Installation” user manual

- Hirschmann Mounting instruction

A.5 IP Parameter Basics

A.5.1 IP Address (Version 4)

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.

Class	Network address	Host address	Address range
A	1 byte	3 Bytes	0.0.0.0 to 127.255.255.255
B	2 Bytes	2 Bytes	128.0.0.0 to 191.255.255.255
C	3 Bytes	1 byte	192.0.0.0 to 223.255.255.255
D			224.0.0.0 to 239.255.255.255
E			240.0.0.0 to 255.255.255.255

Table 11: IP address classes

The first byte of an IP address is the network address. The worldwide leading regulatory board for assigning network addresses is the IANA (Internet Assigned Numbers Authority). If 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

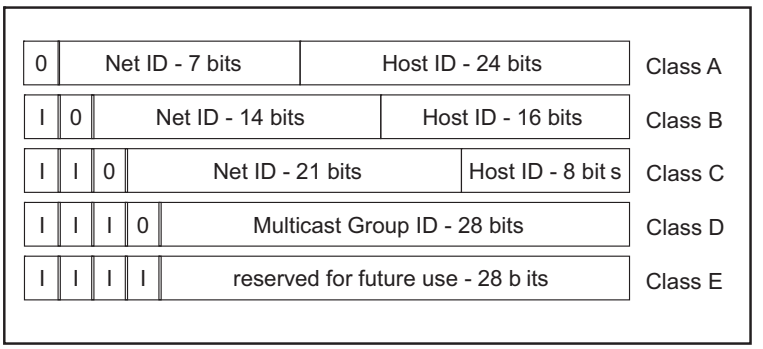


Figure 4: Bit representation of the IP address

The IP addresses belong to class A when their first bit is a zero, for example, the first octet is less than 128.
The IP address belongs to class B if the first bit is a one and the second bit is a zero: for example, the first octet is between 128 and 191.
The IP address belongs to class C when the first 2 bits are a one, for example, the first octet is higher than 191.

Assigning the host address (host ID) is the responsibility of the network operator. The network operator alone is responsible for the uniqueness of the assigned IP addresses.Host address

A.5.2 Netmask

Routers and gateways subdivide large networks into subnetworks. The netmask assigns the IP addresses of the individual devices to a particular subnetwork.

You perform subnetwork division using the netmask in much the same way as the division of the network addresses (net id) into classes A to C.

Set the bits of the host address (host id) that represent the mask to one. Set the remaining host address bits to zero (see the following examples).

Example of a subnet mask:

Decimal notation
255.255.192.0

Binary notation
11111111.11111111.11000000.00000000

Subnetwork mask bits
Class B

Example of IP addresses with subnetwork assignment when applying the subnet mask:

Decimal notation
129.218.65.17

128 < 129 191 › Class B

Binary notation
10000001.11011010.01000001.00010001

Subnetwork 1
Network address

Decimal notation
129.218.129.17

128 < 129 191 › Class B

Binary notation
10000001.11011010.10000001.00010001

Subnetwork 2
Network address

Example of how the network mask is used

In a large network it is possible that gateways and routers separate the management agent from its management station. How does addressing work in such a case?

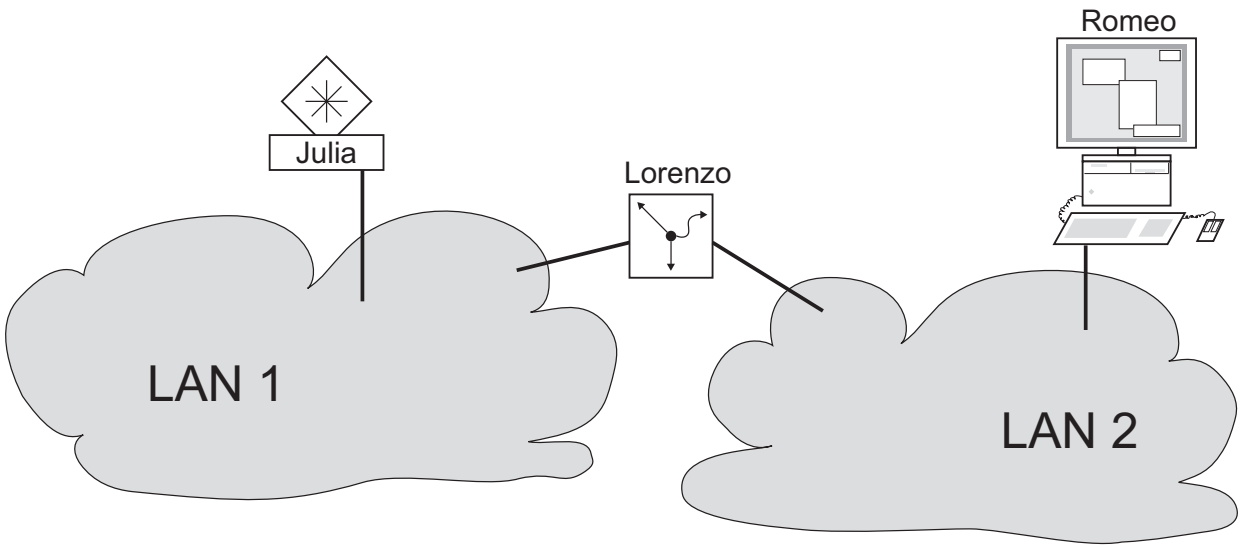


Figure 5: Management agent that is separated from its management station by a router

The 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. This is comparable to going from layer 2 to layer 1, i.e. to sending the data packet over the Ethernet.

Lorenzo receives the letter and removes the outer envelope. From the inner envelope he recognizes 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 when 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 yet another envelope with Lorenzo's MAC destination address.

The letter now travels back to Romeo via Lorenzo, the same way the first letter traveled from Romeo to Juliet.

A.5.3 Classless Inter-Domain Routing

Class C with a maximum of 254 addresses was too small, and class B with a maximum of 65,534 addresses was too large for most users. This resulted 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 for this situation. CIDR overcomes these class boundaries and supports classless IP address ranges.

With CIDR, you enter the number of bits that designate the IP address range. You represent the IP address range in binary form and count the mask bits that designate the netmask. The mask bits equal the number of bits used for the subnet in a given IP address range. Example:

IP address, decimal	Network mask, decimal	IP address, binary
149.218.112.1	255.255.255.128	10010101 11011010 01110000 00000001
149.218.112.127		10010101 11011010 01110000 01111111

25 mask bits

CIDR notation: 149.218.112.0/25

Mask bits

The term “supernetting” refers to combining a number of class C address ranges. Supernetting enables you to subdivide class B address ranges to a fine degree.

A.6 Basics of the Dynamic Host Configuration Protocol (DHCP)

The DHCP (Dynamic Host Configuration Protocol) is a further development of BOOTP, which it has replaced. DHCP additionally allows the configuration of a DHCP client via a name instead of via the MAC address.
For DHCP, this name is known as the “client identifier” in accordance with RFC 2131.
The device uses the name entered under sysName in the system group of the MIB II as the client identifier. You can enter this system name in the `Basic Settings > System` dialog, in the "Device Name" field.

The device sends its system name to the DHCP server. The DHCP server then uses the system name to allocate an IP address as an alternative to the MAC address.

In addition to the IP address, the DHCP server sends

- the netmask
- the default gateway (if available)
- the tftp URL of the configuration file (if available).

The device applies the configuration data to the appropriate parameters. When the DHCP server assigns the IP address, the device saves the configuration data in the non-volatile memory.

Option	Meaning
1	Subnet Mask
2	Time Offset
3	router
4	Time Server
12	Host Name
42	NTP Server

Table 12: DHCP options which the device requests

Option	Meaning
61	Client Identifier
66	TFTP Server Name
67	Bootfile Name

Table 12: DHCP options which the device requests

The advantage of using DHCP instead of BOOTP is that the DHCP server can restrict the validity of the configuration parameters (“Lease”) to a specific time period (known as dynamic address allocation). Before this period (“Lease Duration”) elapses, the DHCP client can attempt to renew this lease. Alternatively, the client can negotiate a new lease. The DHCP server then allocates a random free address.
To help avoid this, DHCP servers provide the explicit configuration option of assigning a specific client the same IP address based on a unique hardware ID (known as static address allocation).

A.7 Basics of the Spanning Tree Protocol

Note: The Spanning Tree Protocol is a protocol for MAC bridges. For this reason, the following description uses the term bridge for GECKO.

Local networks are getting bigger and bigger. This applies to both the geographical expansion and the number of network subscribers. Therefore, it is advantageous to use multiple bridges, for example:

- to reduce the network load in sub-areas,
- to set up redundant connections and
- to overcome distance limitations.

However, using multiple bridges with multiple redundant connections between the subnetworks can lead to loops and the loss of communication through the network. In order to help avoid this, you have the option of using Spanning Tree. Spanning Tree enables loop-free switching through the systematic deactivation of redundant connections. Redundancy helps ensure the systematic reactivation of individual connections as needed.

RSTP is a further development of the Spanning Tree Protocol (STP) and is compatible with it. If a connection or a bridge is inoperable, the STP required a maximum of 30 seconds to reconfigure. This is no longer acceptable in time-sensitive applications. RSTP achieves average reconfiguration times of less than a second. When you use RSTP in a ring topology with 10 to 20 devices, you can even achieve reconfiguration times in the order of milliseconds.

Note: RSTP reduces a layer 2 network topology with redundant paths into a tree structure (Spanning Tree) that does not contain any more redundant paths. One of these takes over the role of the root bridge here. You can specify the maximum number of devices permitted in an active branch from the root bridge to the tip of the branch using the variable `Max Age` for the current root bridge. The preset value for `Max Age` is 20, which can be increased up to 40.
If the device working as the root is inoperable and another device takes over its function, the `Max Age` setting of the new root bridge determines the maximum number of devices allowed in a branch.

Note: The RSTP standard dictates that the devices within a network work with the (Rapid) Spanning Tree Algorithm. If STP and RSTP are used at the same time, the advantages of faster reconfiguration with RSTP are lost in the network segments that are operated in combination.
A device that only supports RSTP works together with MSTP devices by not assigning an MST region to itself, but rather the CST (Common Spanning Tree).

A.7.1 Basics

Because RSTP is a further development of the STP, the following descriptions of the STP also apply to the RSTP.

- The tasks of the STP
  The Spanning Tree algorithm reduces network topologies that are set up using bridges, and that have ring structures with redundant connections, to a tree structure. In doing this, STP divides up the ring structures on the basis of specified rules by deactivating redundant paths. If a path is interrupted because a network component is inoperable, the STP

reactivates the path previously deactivated. This enables redundant connections to increase the communication availability.
In forming the tree structure, the STP determines a bridge that represents the basis of the STP tree structure. This bridge is known as the root bridge.

Features of the STP algorithm:

- automatic reconfiguration of the tree structure in the case of a bridge is inoperable or the interruption of a data path
- stabilization of the tree structure up to the maximum network extension
- stabilization of the topology within a foreseeable time
- topology can be predetermined and reproduced by the administrator
- transparency for the terminal devices
- low network load relative to the available transmission capacity due to the tree structure created

The bridge parameters

Every bridge and its connections are clearly described by the following parameters in the context of Spanning Tree:

- Bridge identifier
- Root path costs of the bridge ports
- Port identifier

Bridge Identifier

The bridge identifier consists of 8 bytes. The 2 highest-value bytes are the priority. The default setting for the priority number is 32,768 (8000H), but the Management Administrator can change this when configuring the network. The 6 lowest-value bytes of the bridge identifier are the MAC address of the bridge. The MAC address enables every bridge to have a unique bridge identifier.
The bridge with the smallest number for the bridge identifier has the highest priority.

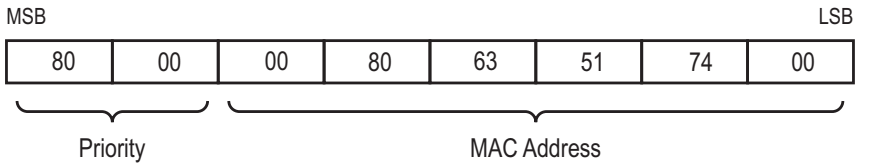


Figure 6: Bridge identifier, example (values in hexadecimal notation)

Root Path Costs

To every path that connects 2 bridges, the bridges assign costs for the transmission (path costs). The bridge determines this value based on the data rate (see table 13). It assigns the higher path costs to paths with lower data rates.

Alternatively, the Administrator can specify the path costs. Like the bridge, the Administrator assigns the higher path costs to paths with lower data rates. However, since the Administrator can choose this value freely, he has a tool with which he can give a certain path an advantage among redundant paths.

The root path costs are the sum of the individual path costs for the paths along which a data packet travels between the connected port of a bridge and the root bridge.

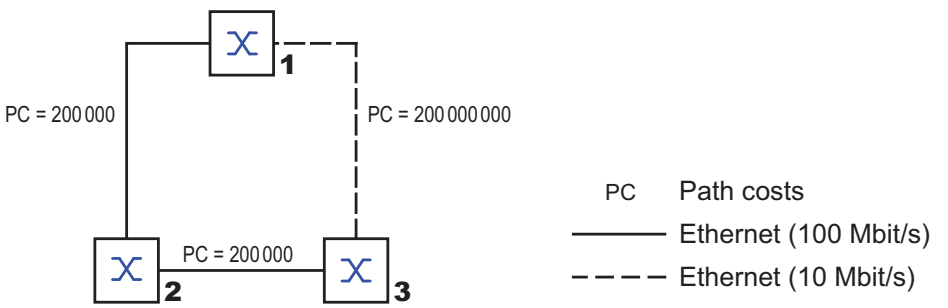


Figure 7: Path costs

Data rate	Recommended value	Recommended range	Possible range
≤100 Kbit/s	[a]	20,000,000-200,000,000	1-200,000,000
1 Mbit/s	20,000,000[a]	2,000,000-200,000,000	1-200,000,000
10 Mbit/s	2,000,000[a]	200,000-20,000,000	1-200,000,000
100 Mbit/s	200,000[a]	20,000-2,000,000	1-200,000,000

Table 13: Recommended path costs for RSTP based on the data rate.

Data rate	Recommended value	Recommended range	Possible range
1 Gbit/s	20,000	2,000-200,000	1-200,000,000
10 Gbit/s	2,000	200-20,000	1-200,000,000
100 Gbit/s	200	20-2,000	1-200,000,000
1 TBit/s	20	2-200	1-200,000,000
10 TBit/s	2	1-20	1-200,000,000

Table 13: Recommended path costs for RSTP based on the data rate.

a. Bridges that conform with IEEE 802.1D 1998 and only support 16-bit values for the path costs should use the value 65,535 (FFFFH) for path costs when they are used in conjunction with bridges that support 32-bit values for the path costs.

Port Identifier

The port identifier consists of 2 bytes. One part, the lower-value byte, contains the physical port number. This provides a unique identifier for the port of this bridge. The second, higher-value part is the port priority, which is specified by the Administrator (default value: 128). It also applies here that the port with the smallest number for the port identifier has the highest priority.

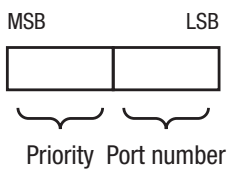


Figure 8: Port identifier

Diameter

The “Max Age” and “Diameter” values largely determine the maximum expansion of a Spanning Tree network.

The number of connections between the devices in the network that are furthest removed from each other is known as the network diameter.

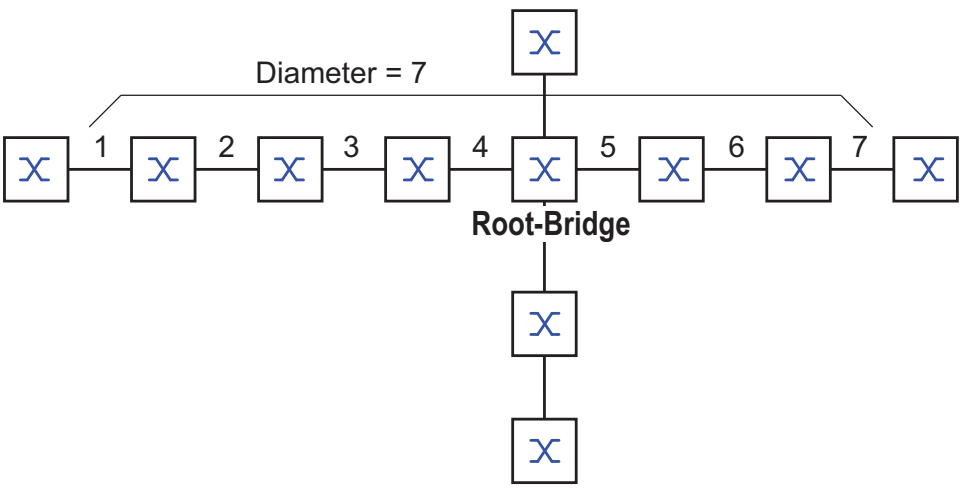


Figure 9: Definition of diameter

The network diameter that can be achieved in the network is MaxAge−1. In the state on delivery, MaxAge is 20 and the maximum diameter that can be achieved is 19. If you set the maximum value of 40 for MaxAge, the maximum diameter that can be achieved is 39.

MaxAge

The “Max Age” and “Diameter” values largely determine the maximum expansion of a Spanning Tree network.

Every STP-BPDU contains a “MessageAge” counter. When a bridge is passed through, the counter increases by 1.
Before forwarding an STP-BPDU, the bridge compares the “MessageAge” counter with the “MaxAge” value defined in the device:

- ☐ If MessageAge < MaxAge, the bridge forwards the STP-BPDU to the next bridge.
- ☐ If MessageAge = MaxAge, the bridge discards the STP-BPDU.

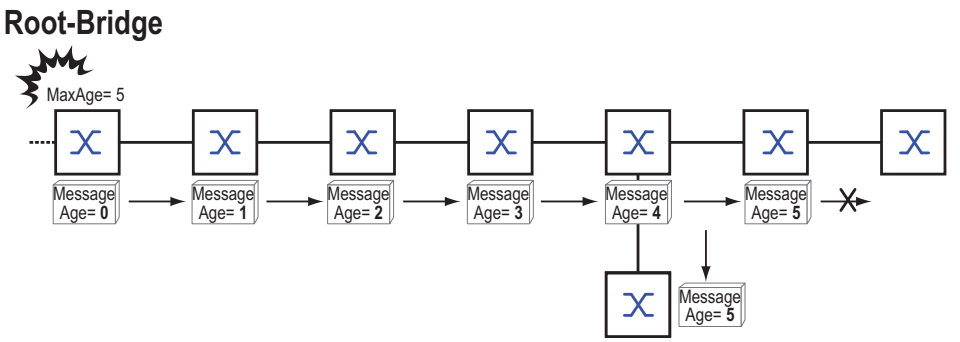


Figure 10: Transmission of an STP-BPDU depending on MaxAge

A.7.2 Rules for creating the tree structure

Bridge information

To calculate the tree structure, the bridges require more detailed information about the other bridges located in the network.
To obtain this information, each bridge sends a BPDU (Bridge Protocol Data Unit) to the other bridges.

The contents of a BPDU include

- bridge identifier,
- root path costs and
- port identifier.

(see IEEE 802.1D).

Setting up the tree structure

- The bridge with the smallest number for the bridge identifier is also known as the root bridge. It is the root of the tree structure.
- The structure of the tree depends on the root path costs. Spanning Tree selects the structure so that the path costs between each individual bridge and the root bridge are kept to a minimum.
- If there are multiple paths with the same root path costs, the bridge furthest away from the root decides which port it blocks. For this purpose, it uses the bridge identifiers of the bridges closer to the root. The bridge blocks the port that leads to the bridge with the numerically higher ID (a numerically higher ID is logically worse). If 2 bridges have the same priority, the bridge with the numerically higher MAC address has the numerically higher ID, and is logically the worse one.
- If multiple paths with the same root path costs lead from one bridge to the same bridge, the bridge further removed from the root uses the port identifier of the other bridge as the last criterion (see figure 8). In the process, the bridge blocks the port that leads to the port with the worse ID. If 2 ports have the same priority, the ID with the higher port number is the worse one.

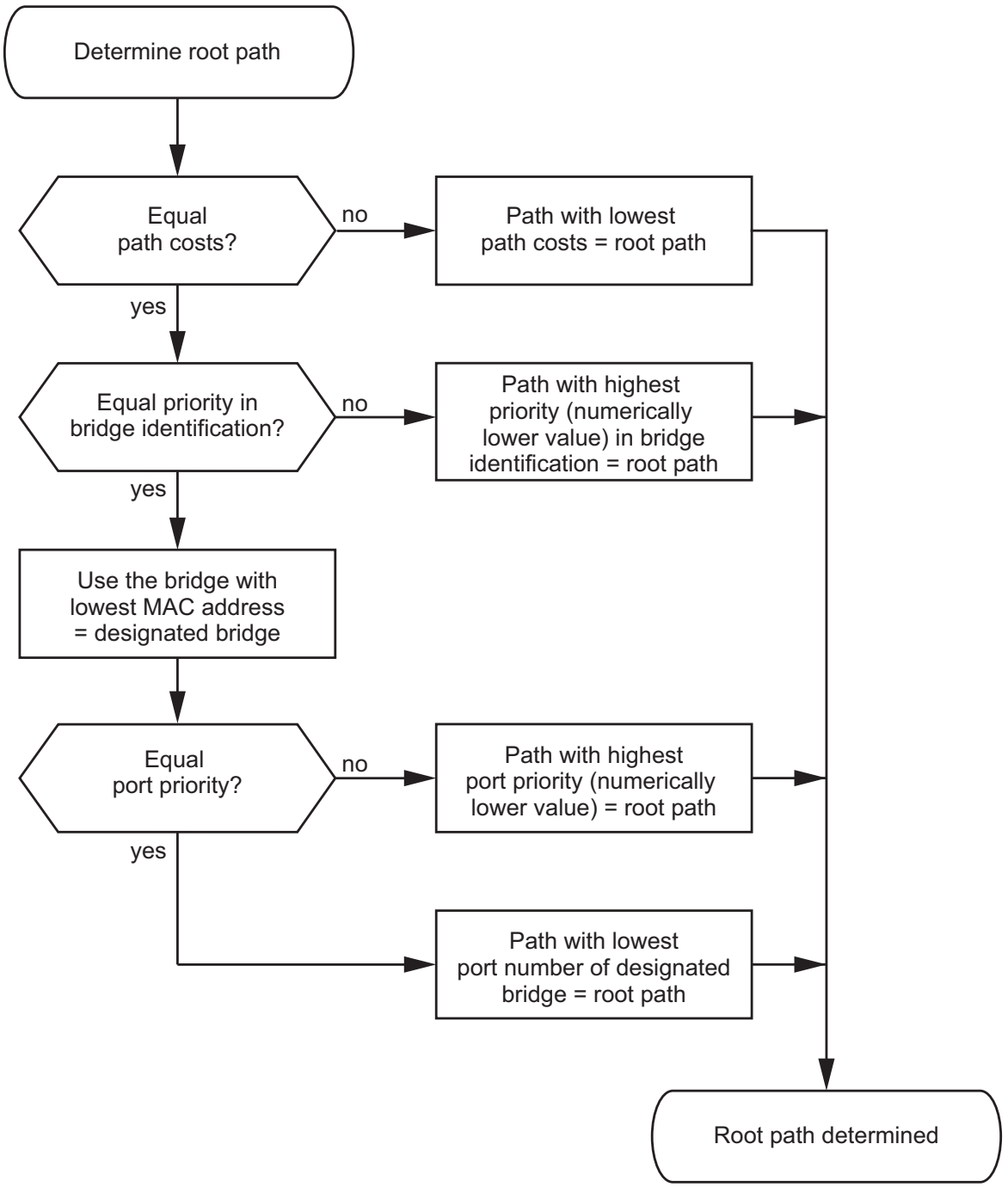


Figure 11: Flow chart for determining the root path

A.7.3 Examples

Example of determining the root path

You can use the network plan (see figure 12) to follow the flow chart (see figure 11) for determining the root path. The administrator has specified a priority in the bridge identifier for each bridge. The bridge with the smallest numerical value for the bridge identifier takes on the role of the root bridge, in this case, bridge 1. In the example the sub-paths have the same path costs. The protocol blocks the path between bridge 2 and bridge 3, as a connection from bridge 3 via bridge 2 to the root bridge would result in higher path costs.

The path from bridge 6 to the root bridge is interesting:

- The path via bridge 5 and bridge 3 creates the same root path costs as the path via bridge 4 and bridge 2.
- STP selects the path using the bridge that has the lowest MAC address in the bridge identifier (bridge 4 in the illustration).
- There are also 2 paths between bridge 6 and bridge 4. The port identifier is decisive here (port 1 < port 3).

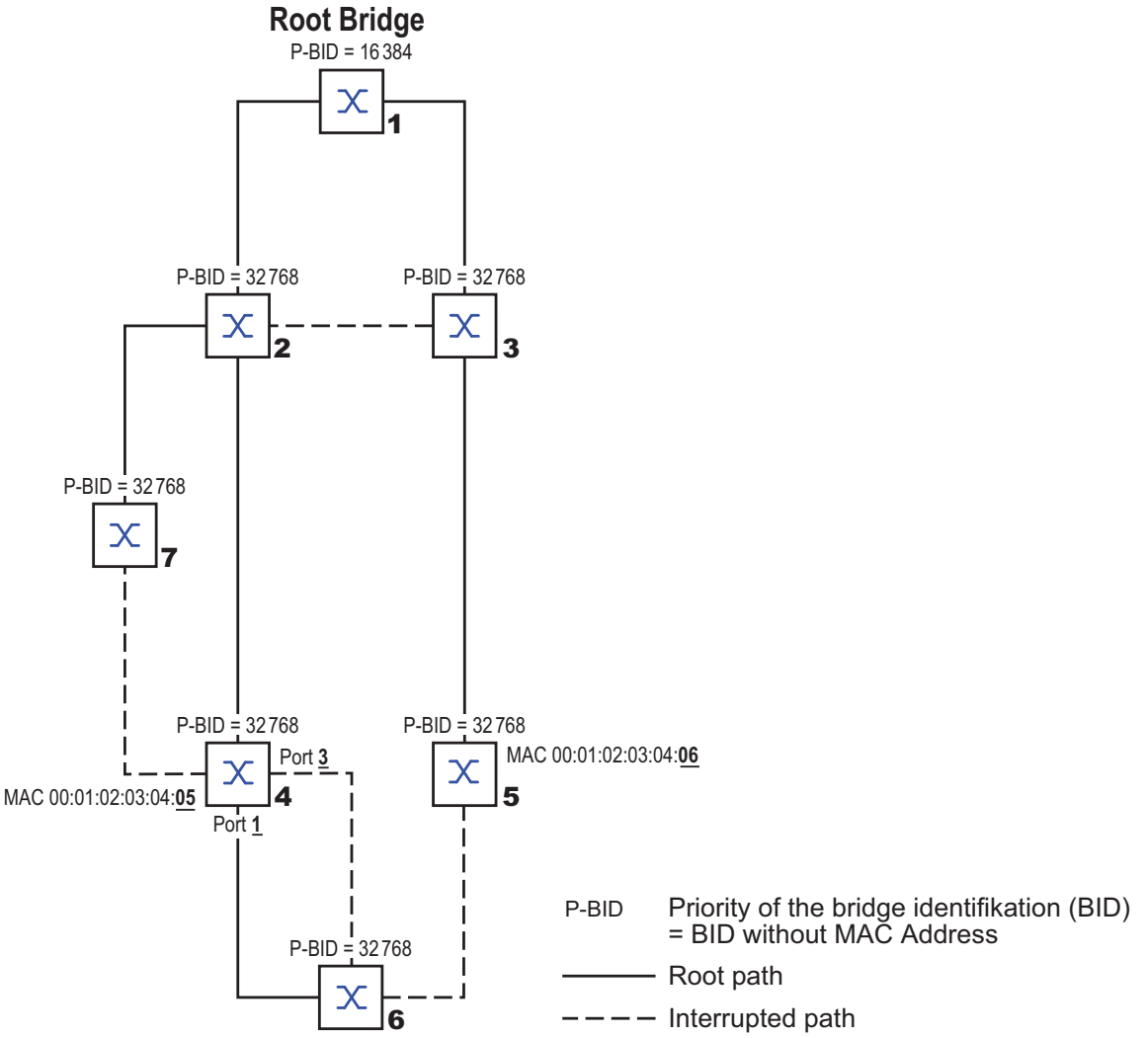


Figure 12: Example of determining the root path

Note: Because the Administrator does not change the default values for the priorities of the bridges in the bridge identifier, apart from the value for the root bridge, the MAC address in the bridge identifier alone determines which bridge becomes the new root bridge if the current root bridge goes down.

Example of manipulating the root path

You can use the network plan (see figure 13) to follow the flow chart (see figure 11) for determining the root path. The Administrator has performed the following:

– Left the default value of 32,768 (8000H) for every bridge apart from bridge 1 and bridge 5 and
– assigned to bridge 1 the value 16,384 (4000H), thus making it the root bridge.
– Assigned to bridge 5 the value 28,672 (7000H).

The protocol blocks the path between bridge 2 and bridge 3, as a connection from bridge 3 via bridge 2 to the root bridge would mean higher path costs.

The path from bridge 6 to the root bridge is interesting:

▶ The bridges select the path via bridge 5 because the value 28,672 for the priority in the bridge identifier is smaller than value 32,768.

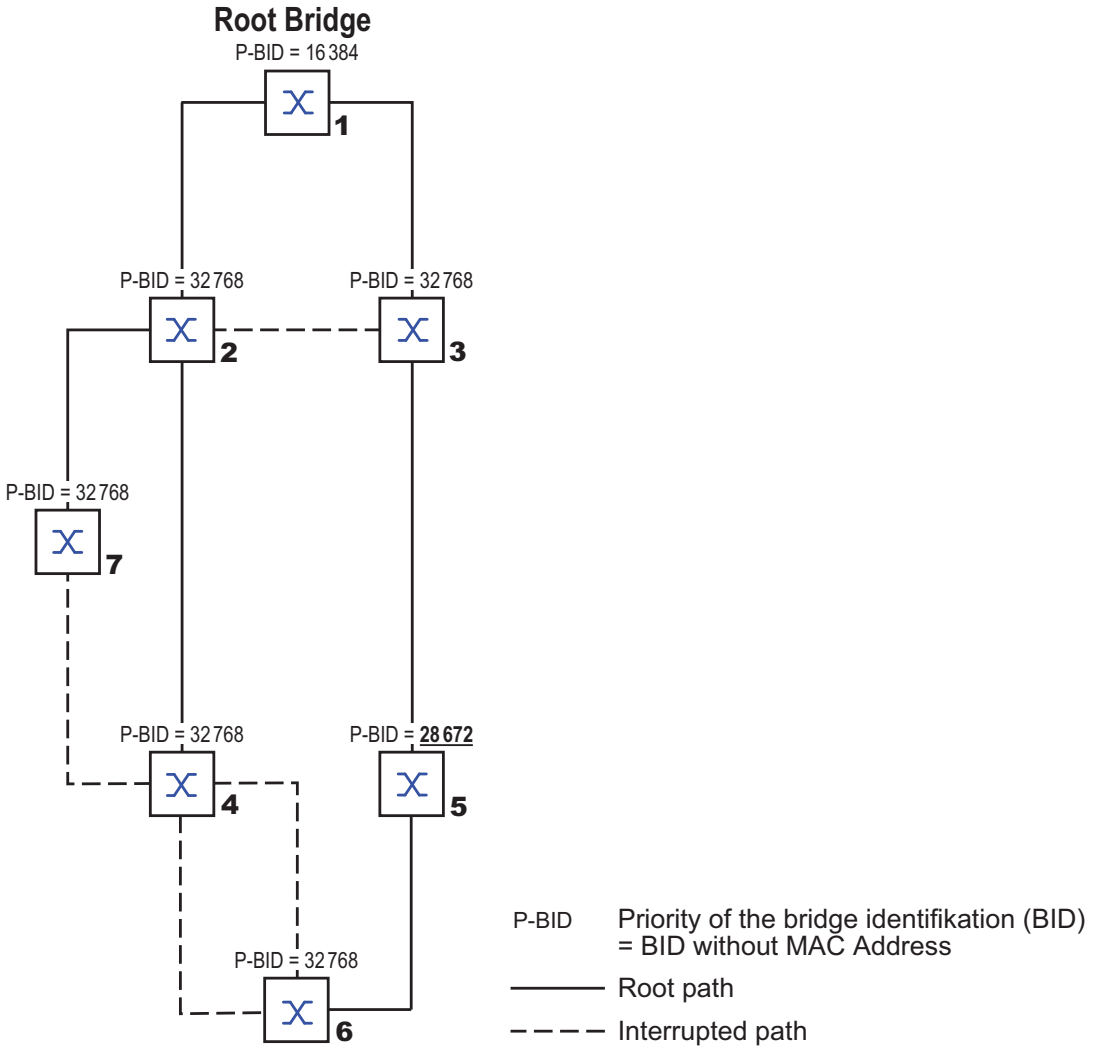


Figure 13: Example of manipulating the root path

Example of manipulating the tree structure

The Management Administrator of the network soon discovers that this configuration with bridge 1 as the root bridge (see on page 162 “Example of determining the root path”) is unfavorable. On the paths from bridge 1 to bridge 2 and bridge 1 to bridge 3, the control packets which the root bridge sends to all other bridges add up.

If the Management Administrator configures bridge 2 as the root bridge, the burden of the control packets on the subnetworks is distributed much more evenly. The result is the configuration shown here (see figure 14). The path costs for most of the bridges to the root bridge have decreased.

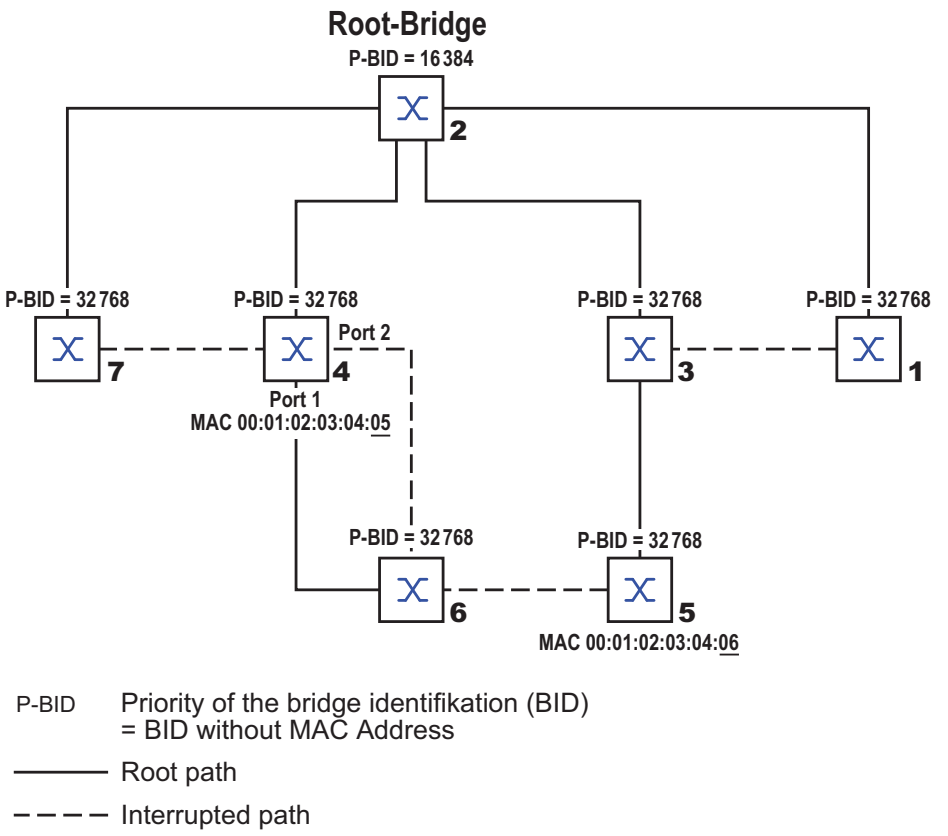


Figure 14: Example of manipulating the tree structure

A.7.4 The Rapid Spanning Tree Protocol

The RSTP takes over the calculation of the tree structure by the STP unchanged. RSTP merely changes parameters, and adds new parameters and mechanisms that speed up the reconfiguration if a connection or a bridge is inoperable.
The ports play a significant role in this context.

- **Port roles**
  RSTP assigns each bridge port one of the following roles (see figure 15):

  - Root Port:
    This is the port at which a bridge receives data packets with the lowest path costs from the root bridge.
    If there are multiple ports with equally low path costs, the bridge ID of the bridge that leads to the root (designated bridge) decides which of its ports is given the role of the root port by the bridge further removed from the root.
    If a bridge has multiple ports with equally low path costs to the same bridge, the bridge uses the port ID of the bridge leading to the root (designated bridge) to decide which port it selects locally as the root port (see figure 11).
    The root bridge itself does not have a root port.
  - Designated Port:
    The bridge in a network segment that has the lowest root path costs is the designated bridge.Designated Bridge).
    If multiple bridges have the same root path costs, the bridge with the lowest numerical bridge identifier takes over the role of the designated bridge. The designated port on this bridge is the port that connects a network segment leading away from the root bridge. If a bridge with more than one port is connected with a network segment (e.g. via a hub), it gives the role of designated port to its port with the better port identifier.
  - Edge Port: [1]:
    Every network segment in which there are no additional RSTP bridges is connected with exactly one designated port. This designated port is then also an edge port if it has not received any BPDUs (Spanning Tree Bridge Protocol Data Units).

1. An edge port is an end device port at the “edge” of a switched network.

- Alternate Port:
  This is a blocked port that takes over the task of the root port if the connection to the root bridge is inoperable. The alternate port helps maintain the connection of the bridge to the root bridge.
- Backup Port:
  This is a blocked port that serves as a backup in case the connection to the designated port of this network segment (without RSTP bridges, e.g. a hub) is inoperable.
- Disabled Port (Disabled Port):
  This is the port that does not play any role within the Spanning Tree protocol, i.e. it is disabled or does not have any connection

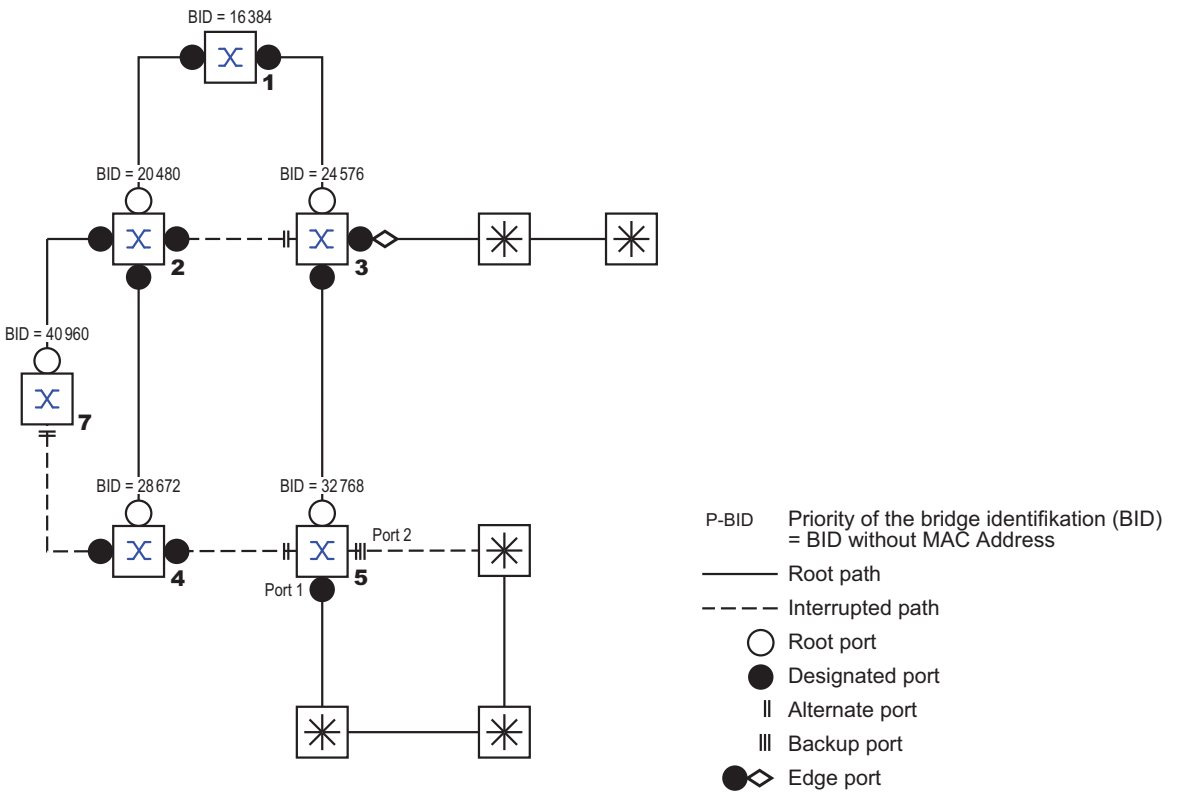


Figure 15: Port role assignment

Port states

Depending on the tree structure and the state of the selected connection paths, the RSTP assigns the ports their states.

STP port state	Administrative bridge port state	MAC Operational	RSTP Port state	Active topology (port role)
DISABLED	Disabled	FALSE	Discarding[a]	Excluded (disabled)
DISABLED	Enabled	FALSE	Discarding[a]	Excluded (disabled)
BLOCKING	Enabled	TRUE	Discarding[b]	Excluded (alternate, backup)
LISTENING	Enabled	TRUE	Discarding[b]	Included (root, designated)
LEARNING	Enabled	TRUE	Learning	Included (root, designated)
FORWARDING	Enabled	TRUE	Forwarding	Included (root, designated)

Table 14: Relationship between port state values for STP and RSTP

a. The dot1d-MIB displays “Disabled”
b. The dot1d-MIB displays “Blocked”

Meaning of the RSTP port states:

- Disabled: Port does not belong to the active topology
- Discarding: No address learning in FDB, no data traffic except for STP-BPDUs
- Learning: Address learning active (FDB), no data traffic apart from STP-BPDUs
- Forwarding: Address learning active (FDB), sending and receiving of all frame types (not only STP-BPDUs)

Spanning Tree Priority Vector

To assign roles to the ports, the RSTP bridges exchange configuration information with each other. This information is known as the Spanning Tree Priority Vector. It is part of the RST BPDUs and contains the following information:

- Bridge identifier of the root bridge
- Root path costs of the sending bridge
- Bridge identifier of the sending bridge
- Port identifier of the port through which the message was sent
- Port identifier of the port through which the message was received

Based on this information, the bridges participating in RSTP are able to determine port roles themselves and define the port status of their local ports.

Fast reconfiguration

Why can RSTP react faster than STP to an interruption of the root path?

- Introduction of edge ports:
  During a reconfiguration, RSTP switches an edge port into the transmission mode after three seconds (default setting) and then waits for the “Hello Time” to elapse, to verify that no bridge sending BPDUs is connected.
  When the user cares about that a terminal device is connected at this port and will remain connected, there are no waiting times at this port in the case of a reconfiguration.
- Introduction of alternate ports:
  As the port roles are already distributed in normal operation, a bridge can switch from the root port to an alternate port after the connection to the root bridge is lost.
- Communication with neighboring bridges (point-to-point connections):
  Decentralized, direct communication between neighboring bridges enables a reaction to status changes without waiting periods in the spanning tree topology.
- Address table:
  With STP, the age of the entries in the FDB determines the updating of the communication. RSTP immediately deletes the entries in those ports that are affected by a reconfiguration.
- Reaction to events:
  Without having to adhere to any time specifications, RSTP immediately reacts to events such as connection interruptions, connection reinstatements, etc.

Note: The downside of this fast reconfiguration is the possibility that data packages could be duplicated and/or arrive at the receiver in the wrong order during the reconfiguration phase of the RSTP topology. If this is unacceptable for your application, use the slower Spanning Tree Protocol or select one of the other, faster redundancy procedures described in this manual.

- STP compatibility mode
  The STP compatibility mode allows you to operate RSTP devices in networks with old installations. If an RSTP device detects an older STP device, it switches on the STP compatibility mode at the relevant port.

A.8 Basics of the Topology Discovery

IEEE 802.1AB describes the Link Layer Discovery Protocol (LLDP). LLDP enables the user to have automatic topology discovery for his LAN.

Devices with active LLDP:

- send their connection and management information to the neighboring devices in the shared LAN. The devices are evaluated when the LLDP function is activated in the receiving device.
- receive connection and management information from neighboring devices in the shared LAN if these devices have also activated LLDP.
- create a database with management information and object definitions on neighboring devices that have also activated LLDP.

A central element of the connection information is the exact, unique ID of the connection point: MAC (service access point): This is made up of a device ID unique within the network and a port ID unique for this device.
Content of the connection and management information:

- Chassis ID (its MAC address)
- Port ID (its port MAC address)
- Description of the port
- System name
- System description
- Supported system functions
- Currently active system functions
- Interface ID of the management address
- VLAN ID of the port
- Status of the autonegotiation at the port
- Setting for medium/half and full duplex and for the port speed.
- Information about the VLANs installed on the device (VLAN ID and VLAN name, regardless of whether the port is a VLAN member).

A network management station can call up this information from devices with LLDP activated. This information enables the network management station to map the topology of the network.

802.1d devices normally block the special multicast LLDP IEEE MAC address used for information exchange. For this reason, non-LLDP devices discard LLDP packets. When a non-LLDP-capable device is positioned between 2 LLDP-capable devices, the non-LLDP-capable device prohibits information exchange between the 2 LLDP-capable devices.

The Management Information Base (MIB) for an LLDP-capable device holds the LLDP information in the LLDP MIB.

A.9 Basics of prioritizing the data traffic

A.9.1 Description of prioritization

For data traffic prioritization, traffic classes are predefined in the device. The device prioritizes higher traffic classes over lower traffic classes.

To provide for optimal data flow for delay-sensitive data, you assign higher traffic classes to this data. You assign lower traffic classes to data that is less sensitive to delay.

Assigning traffic classes to the data

The device automatically assigns traffic classes to inbound data (traffic classification). The device takes the following classification criteria into account:

- Methods according to which the device carries out assignment of received data packets to traffic classes:
  - `trustDot1p`:The device uses the priority of the data packet contained in the VLAN tag.
  - `trustIpDscp`:The device uses the QoS information contained in the IP header (ToS/DiffServ).
  - `untrusted`:The device ignores possible priority information within the data packets and uses the priority of the receiving port directly.
- The priority assigned to the receiving port.

Both classification criteria are configurable.

Prioritizing traffic classes

For the prioritization of traffic classes, the device uses the method "Strict":

When the data of a higher traffic class is no longer being sent, or the relevant data is still in the queue, the device sends data of the corresponding traffic class. If all traffic classes are prioritized according to the “strict” method, when there is a high network load the device may block the data of lower traffic classes.

A.9.2 Handling of received priority information

Applications label data packets with the following prioritization information:

- VLAN priority based on IEEE 802.1Q/ 802.1D (Layer 2)
- Type-of-Service (ToS) or DiffServ (DSCP) for VLAN Management IP packets (Layer 3)

The device offers the following options for evaluating this priority information:

- `trustDot1p`
  The device assigns VLAN-tagged data packets to the different traffic classes according to their VLAN priorities. The corresponding assignment is configurable. The device assigns the priority of the receiving port to data packets that it receives without a VLAN tag.
- `trustIpDscp`
  The device assigns the IP packets to the different traffic classes according to the DSCP value in the IP header, even if the packet was also VLAN-tagged. The corresponding assignment is configurable. The device prioritizes non-IP packets according to the priority of the receiving port.
- `untrusted`
  The device ignores the priority information in the data packets and assigns the priority of the receiving port to the packets.

A.9.3 VLAN tagging

For the VLAN and prioritizing functions, the IEEE 802.1Q standard provides for integrating a VLAN tag into the MAC data frame. The VLAN tag consists of 4 bytes and is located between the source address field (“Source Address Field”) and the type field (“Length / Type Field”).

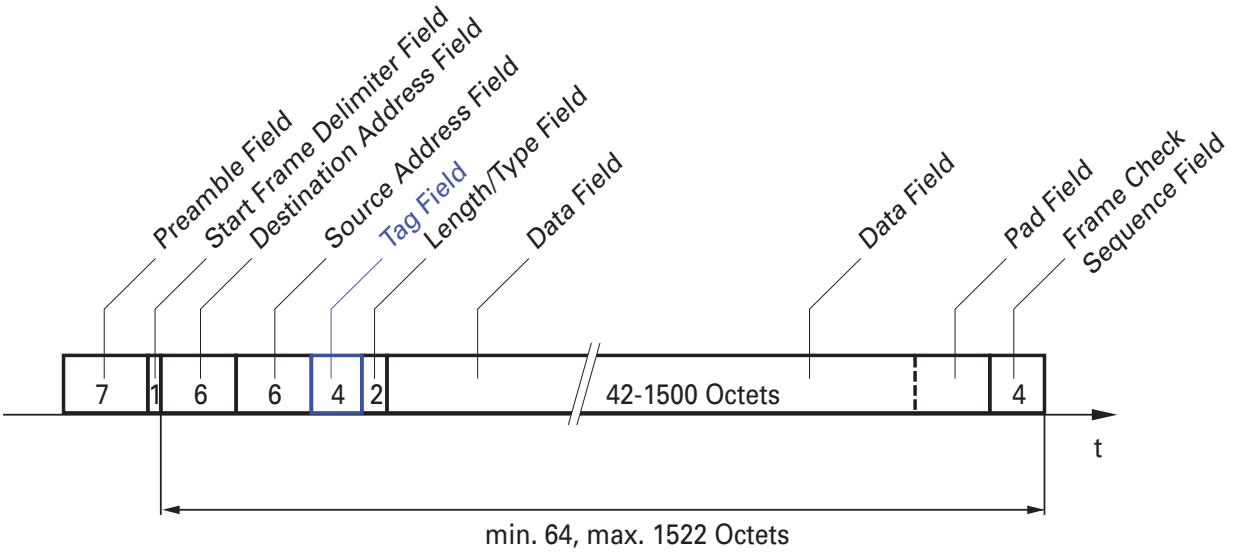


Figure 16: Ethernet data packet with tag

For data packets with VLAN tags, the device evaluates the priority information.

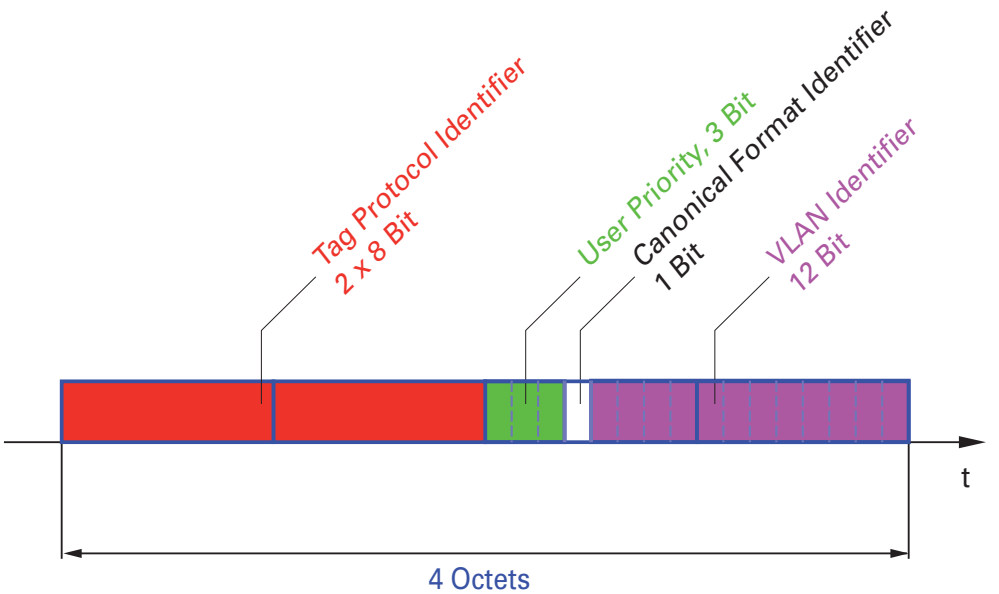


Figure 17: Structure of the VLAN tagging

Data packets with VLAN tags containing priority information but no VLAN information (VLAN ID = 0) are known as Priority Tagged Frames.

Note: Network protocols and redundancy mechanisms use the highest traffic class 7. Therefore, you select lower traffic classes for application data.

When using VLAN prioritizing, consider the following special features:

- End-to-end prioritization requires universal transmission of VLAN tags in the entire network. The prerequisite is that each participating network component is VLAN-capable.
- Routers are not able to send and receive packets with VLAN tags via port-based router interfaces.

A.9.4 Handling of traffic classes

Description of Strict Priority

With the Strict Priority setting, the device first transmits the data packets that have a higher traffic class (higher priority) before transmitting a data packet with the next highest traffic class. The device transmits a data packet with the lowest traffic class (lowest priority) only when there are no other data packets remaining in the queue. In unfortunate cases, the device does not send packets with a low priority if there is a high volume of high-priority traffic waiting to be sent on this port.
In delay-sensitive applications, such as VoIP or video, Strict Priority allows high priority data to be sent immediately.

A.10 Basics of flow control

If a large number of data packets are received in the sending queue of a port at the same time, this can cause the port memory to overflow. This happens, for example, when the device receives data on a Gigabit port and forwards it to a port with a lower bandwidth. The device discards surplus data packets.

The flow control mechanism described in standard IEEE 802.3 helps ensure that no data packets are lost due to a port memory overflowing. Shortly before a port memory is completely full, the device signals to the connected devices that it is not accepting any more data packets from them.

- In full duplex mode, the device sends a pause data packet.
- In half duplex mode, the device simulates a collision.

The following figure shows 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. As a result, the receiving queue of port 4 overflows. The left funnel symbolizes this status.

If the flow control function at ports 1, 2 and 3 of the device is turned on, the device reacts before the funnel overflows. The funnel on the right side represents ports 1, 2 and 3, which send a message to the transmitting devices in order to control the transmission speed. As a result of this, the receiving port is no longer overloaded and is able to process the incoming traffic.

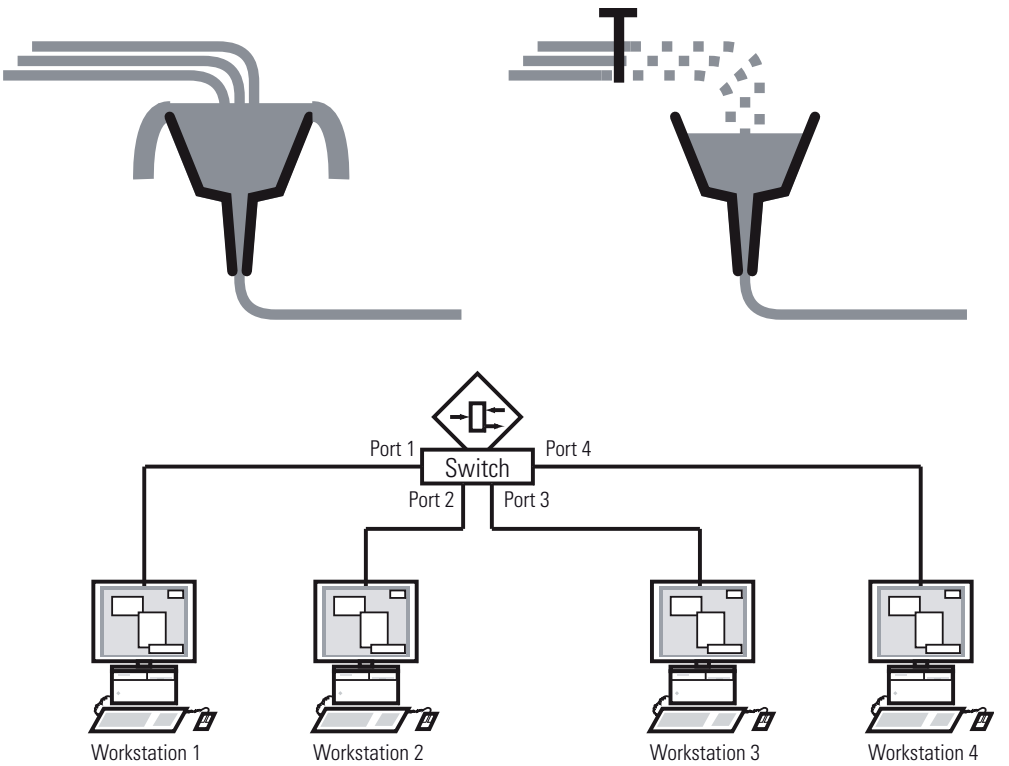


Figure 18: Example of flow control

A.10.1 Half duplex or full duplex link

- **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, which detects a collision and interrupts the sending process.

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 take a small break in the sending transmission.

A.11 Basics of the Management Information Base MIB

The Management Information Base (MIB) is designed as an abstract tree structure.
The branching points are the object classes. The “leaves” of the MIB are known as generic object classes.
If this is required for unique identification, the generic object classes are instantiated, i.e. the abstract structure is mapped onto reality, for example 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. Therefore, the instance “`get 1.3.6.1.4.1.248.11.11.1.1.1.1.2.1`” supplies “1” as a response, meaning that the power supply is ready for operation.

Definition of the syntax terms used:	
Integer	A whole number 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… (e.g. 1.3.6.1.4.1.248…)
Octet string	ASCII character string
PSID	Power supply identifier (number of the power supply unit)

Definition of the syntax terms used:	
TimeTicks	Stopwatch Elapsed time (in seconds) = numerical value/100 Numerical value = integer in the range $0\text{-}2^{32}\text{-}1$
Timeout	Time value in hundredths of a second Time value = integer in the range $0\text{-}2^{32}\text{-}1$
Type field	4-digit hexadecimal number in accordance with ISO/IEC 8802-3
Counter	Integer ($0\text{-}2^{32\text{-}1}$) whose value is incremented by 1 when specific events occur.

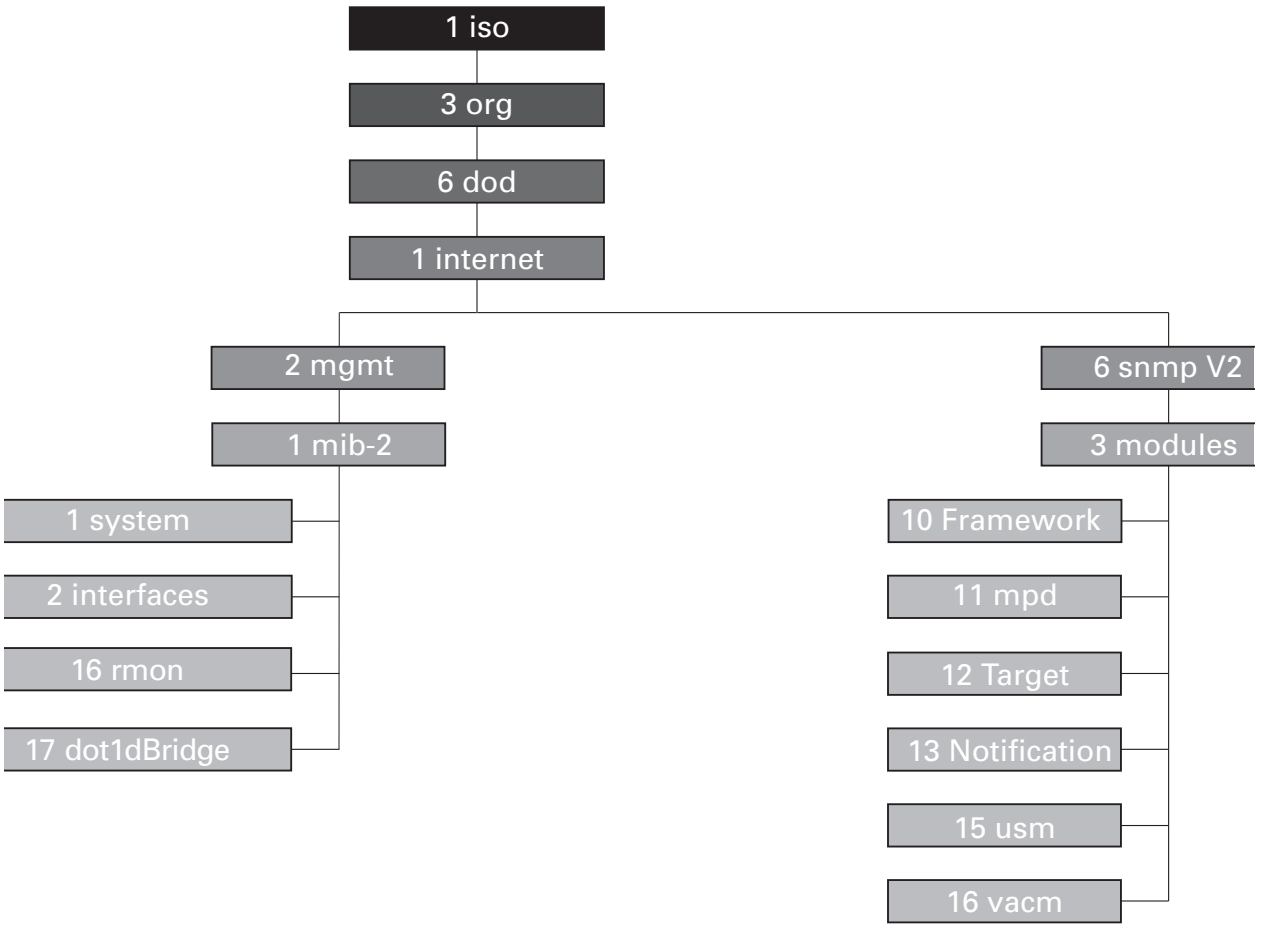


Figure 19: Tree structure of Hirschmann MIB GECKO 4TX

A.12 Copyright of integrated software

A.12.1 Included open source software

This product includes the follwing open source software originated from third parties that is subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL).

- BusyBox
- Open-LLDP
- Log Writer Library (LWL)
- rstplib
- U-Boot
- tinytest
- Linux

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change freesoftware--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit tousing it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights.

These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.
For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below,refers to any such program or work, and a "work based on the Program"means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on theProgram (independent of having been made by running the Program).Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty;and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portionof it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program,and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works.

But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume ofa storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it,under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not includeanything that is normally distributed (in either source or binaryform) with the major components (compiler, kernel, and so on) of theoperating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues),conditions are imposed on you (whether by court order, agreement orotherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW.

EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BYYOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail. If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or yourschool, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program intoproprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library.Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU LesserGeneral Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.
We call this license the "Lesser" General Public License because itdoes Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In thiscase, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body offree software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License").Each licensee is addressed as "you".
A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on theLibrary" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilationand installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool forwriting it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with theLibrary.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portionof it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)
These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works inthemselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms ofthis License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.
In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General PublicLicense instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Librarycreates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)
Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6,whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do oneof these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses theLibrary" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.
It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based onthe Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on theLibrary), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifyingthe Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time.Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
Each version is given a distinguishing version number. If the Libraryspecifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free statusof all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW.EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OROTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANYKIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THEIMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULARPURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THELIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THELIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS
How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>
This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or yourschool, if any, to sign a "copyright disclaimer" for the library, ifnecessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990 Ty Coon, President of Vice

That's all there is to it!

Note: The software included in this product contains copyrighted software that is licensed under the GPL and LGPL. You may obtain the complete corresponding source code from us for a period of three years after our last shipment of this product by sending a request to:

Hirschmann Automation and Control GmbH
3rd Level Support
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany

A.13 Abbreviations

ACA	AutoConfiguration Adapter
ACL	Access Control List
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
FDB	Forwarding Database
GUI	Graphic user interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
F/O	Optical Fiber
MAC	Media Access Control
MIB	Management Information Base
MRP	Media Redundancy Protocol
MSTP	Multiple Spanning Tree Protocol
NMS	Network Management System
NTP	Network Time Protocol
PC	Personal Computer
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RSTP	Rapid Spanning Tree Protocol
SCP	Secure Copy
SFP	Small Form-factor Pluggable
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TP	Twisted Pair
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

B Readers' Comments

What is your opinion of this manual? We are always striving to provide as comprehensive a description of our product as possible, to help ensure trouble-free operation. 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
Completeness	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 no.:

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
- by post to

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

C Further support

Technical questions

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

You find the addresses of our partners on the Internet at https://www.hirschmann.com.

A list of local telephone numbers and email addresses for technical support directly from
Hirschmann is available at https://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
https://www.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
  https://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.

HIRSCHMANN

A BELDEN BRAND