Pushing Performance

People | Power | Partnership

HARTING Ha-VIS Management Software mCon 3000 Next Generation

User Manual Web Interface

3rd Edition 2013, revised 10/13

Author: HARTING
Scriptor Dokumentations Service GmbH
Editor: HARTING

Printed on bleached cellulose. 100% free from chlorine and acid.

Figures

1. Introduction

HARTING's family Ha-VIS mCon of managed Ethernet switches are suitable for creating Ethernet, Fast Ethernet and Gigabit Ethernet networks (up to 1000 Mbit/s) with distributed star or nodal points in industrial environments where a high level of operational reliability is required.

Equipped with up to ten ports, the Ethernet switch can be mounted directly in the field for convenient networking of Ethernet devices. Your HARTING Ha-VIS mCon Ethernet Switch comes with an embedded web server and a user-friendly web interface that makes switch management intuitive and efficient. Configuration and maintenance are also possible using SNMP versions 1, 2 and 3 or using the Command Line Interface (CLI) via Telnet or ssh.

This software guide for the Ha-VIS mCon family of switches contains information required to operate the switch management software. This information is applicable for all switches in the Ha-VIS mCon 3000 NG series. The examples and screenshots in this manual are taken from the Ha-VIS mCon 3102-AASFP; the number of ports and the information shown in your software may vary depending on the model of switch you use.

This software guide has the following structure:

Chapters 1 to 3	Notes on safety and general information about this manual
Chapters 4 and 5	Basic information about the software, user rights, installation and logging in
Chapters 6 to 18	Details about the software's areas and windows and the settings that can be made
Chapters 19 to 20	Information about SD Memory Card and other service
Appendix	Glossary of terms and abbreviations, index

2. Safety Guidelines and Approved Usage

In order to function properly, the switch management software must be correctly installed and appropriately operated. The switch management software should be used only in conjunction with a HARTING Ethernet switch.

Observe the following general safety instructions before installing and using the switch management software:

- Ensure correct polarity and voltage when connecting the power supply to the Ethernet switch.
- Use only shielded cable for data lines.
- Use only cables that comply with the corresponding standards for Ethernet connections.

ATTENTION

The Ethernet switch should be operated only when it is properly and securely mounted.

CAUTION

Only authorized and qualified personnel are permitted to work on this device!
Improper work or repairs can damage the integrated protective safety functions and the performance of this device. This can cause the device to malfunction, be a source of personal danger, or cause damage to connected machines or connected systems.

3. General Notes about this Manual

3.1 Explanation of the symbols

The following symbols are used in this software guide:

CAUTION

This symbol describes warning notes that indicate a low-level source of danger. If not avoided, light or minor injuries or damage to property may result.

ATTENTION

This word describes warning notes that indicate a low-level source of danger. If not avoided, damage to property may result.

Note

This symbol describes general notes that provide important information concerning one or more operating steps. Such notes may also provide references to further information supplied within this manual.

3.2 Typographical conventions

This manual uses the following typographical conventions to describe the software interface:

Italics — Text in italic font refers to an entered value, a selection from a drop-down list (such as *Enable*), a reference to a section of the software menu (such as *System Settings → General Settings*) or drop-down list choices.

Bold — Text in bold font refers to the name of a row or column found within the software interface, or to the name of a field where data is displayed or specified.

3.3 Additional information

Mounting instructions for this switch can be found in the *Installation Notes* included in the delivery. The *Installation Notes* also provide valuable hardware-specific information such as the pin-out assignments, LED displays, technical specifications, and power supply requirements.

The latest versions of the switch firmware and the manual can be downloaded from the Internet at http://www.HARTING.com.

4. Basic Operation

Make sure that the switch is securely mounted before starting any software configuration. Refer to the *Installation Notes* for mounting instructions.

This Ethernet switch must first be connected to your local area network before it can be configured. The switch management software and the embedded web server are pre-installed on the switch.

You will require a networked computer with an HTTP web browser or an SNMP Tool to configure the switch management software. Optionally you can also install a TFTP server program on this PC in the event that you need to update the switch firmware or export respectively import a configuration file.

4.1 Switch access and configuration

The Ha-VIS mCon switches offer a variety of software functionalities to configurate and set up the network. For configuration purpose, the switch can be accessed in several ways.

The easiest way is to use a standard web browser to configurate the switch via a graphical HTTP based user interface. To connect to the switch, the user must log in to the switch using the web browser (following the instructions below). The user must log out before exiting the browser, because the parallel connections to the switch (web sessions) are limited to two and the timeout for each session is 10 minutes. Once you logged out, you can close the browser window in which the web interface was running.

The second way is to access the switch via an SNMP software. The Ha-VIS mCon Ethernet Switches are supporting the standard MIB II and can be easily integrated to an existing LAN infrastructure and management suite. Some functionalities are product and HARTING specific and therefore are not included in the MIB II. To get also access to this functionalities using SNMP, you have to copy the HARTING MIB file to your MIB repository of your SNMP software.

The third way of configuring the switches is to use the command line interface (CLI). The CLI can be accessed using the network protocols TELNET or SSH. Most operating systems are equipped with a TELNET client. Alternatively clients like PuTTY can be used. After logging in to the system, you will reach the prompt to enter the commands for configuring the switch. For detailed information on how to use the command line interface, refer to the CLI manual.

4.2 Web access

4.2.1 Logging in

Proceed as follows to turn on the switch and to login in:

1. Connect the switch to your network or to a service computer using an Ethernet patch cable. You may select any free port on the switch.
2. Connect the switch to the power supply (refer to the *Installation Notes*). The switch will take about thirty seconds to boot up.
3. Turn on a computer connected to the same network as the switch. If you are starting with a brand new switch, you should initially configure your host PC so that it is on the same network segment as the switch (the switch has a factory default IP of *192.168.0.126*, and a subnet mask of *255.255.255.0*).
4. Start your web browser or open a new browser window.

5. Enter the network address of the switch into the browser. See the *Installation Notes / Quick Start Guide* for more information about altering your computer's network settings. The *Login Screen* of the software will be displayed after your browser has successfully established an HTTP connection to the switch.
6. Enter your username and password. Normally, the *admin* account is used for switch administration. A *guest* account exists for viewing the configuration only. The default *admin* password is *harting*. You should change this password as soon as possible.

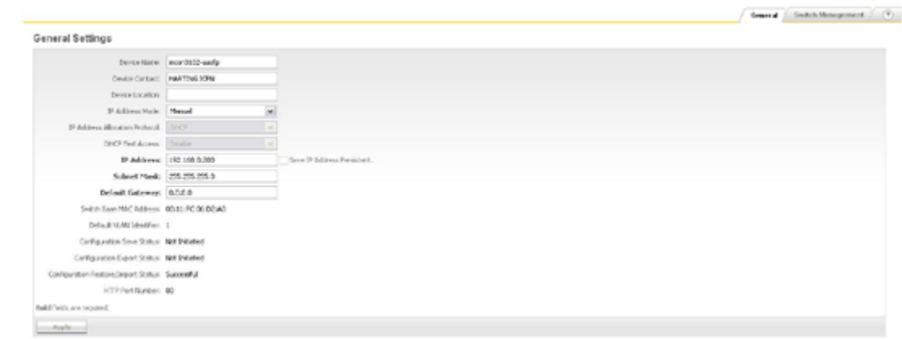


Figure 4-1 General Settings

4.2.2 Logging out

To log out from the software at any time, simply click the *Logout* button in the top right-hand task bar. The *Login Screen* is then once again displayed.

4.3 SNMP configuration

To get access to the switch using SNMP, an SNMP based software tool is needed. SNMP (Simple Network Management Protocol) is the most widely-used network management protocol on TCP/IP-based networks. SNMP provides an easy mechanism for managing a network using a simple Command-Response protocol defined between the Manager and the managed entities. The management is performed through MIBs (Management Information Base) supported by the managed entities. The MIBs contain configuration elements, which can be either Viewed (GET) or Modified (SET) by the Managers.

To access the switch, you need the following information:

- Switch IP address (**Default value:** *192.168.0.126*)
- Community password to read values from the switch (**Default value:** *public*)
- Community password to read/write values from/to the switch (**Default value:** *private*)

For additional information refer to mCon 3000 NG User Manual SNMP.

5. Multifunction Button

Via the *Multifunction Button* (MFB) the customer is able to set some specific parameters of the switch, without accessing it via Web or SNMP.

This chapter describes how to use the MFB and the Service Mode.

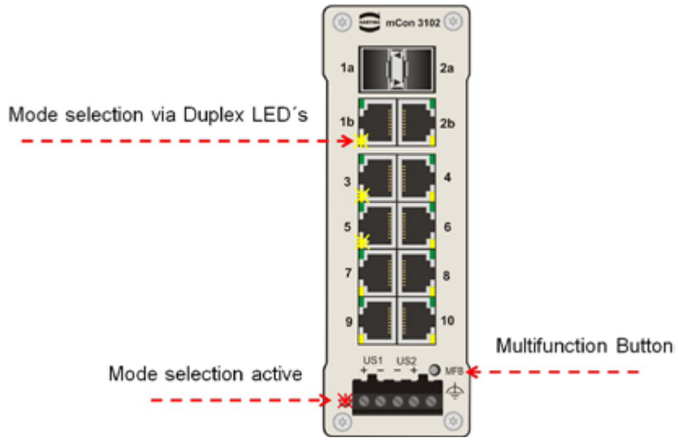


Figure 5-1 Operating the Multifunction Button

Operation sequence:

The operation of the MFB is available after the switch has finished the boot up.

The selection of each function is displayed via the 100 Mbit/s LEDs.

If the MFB is pressed the first time (first press 3 sec), the yellow LEDs for displaying the 100 Mbit/s mode are disabled for all ports and the red *Fault* LED is lit continuously to show that the configuration via the button is possible.

After pressing the button for the first time, the 100 Mbit/s LED on port 1 is lit and the function (Reboot) is selected.

When the button is pressed for a second time, the LED of port 2 is lit and the second mode is selected.

Select the function by tapping the MFB an according number of times. Now, the switch is waiting three seconds for further commands. The selection will be confirmed by two flashes of the red Fault LED.

Should no action be executed, the MFB must be pressed until all 100 Mbit/s LEDs are off and the switch returns to normal operation (red *Fault* LED off again).

#	Function	Description
1	Reboot	Hardware reset
2	Set DHCP	Sets the IP address mode to DHCP
3	Set static IP	Sets the IP address to 192.168.0.126 and subnet mask to 255.255.255.0
4	Enable PROFINET	Enables PROFINET
5	Disable PROFINET	Disables PROFINET
6	Reset to factory defaults	Sets the switch to factory default settings
7	Reset to factory defaults, keep IP	Set the switch to factory default settings with the exception of the IP address

6. Introduction to the Web Browser Interface

The web interface offers a simple way to manage the software functionalities of the Ha-Vis mCon Ethernet Switches. The websites will be refreshed automatically in short intervals.

One of the following web browser versions should be used for switch configuration:

- Microsoft Internet Explorer version 7 or later
- Firefox version 2 or later

6.1 The menus

The structure of the software interface has been kept simple. After logging in to the mCon homepage, you will see a main navigation menu tree on the left side and an active window in the middle right side of the browser window. Using the menu tree, you can access all of the settings and statistics available on the switch. On the top you find the options for refreshing the window or to logout form the web interface. The menu bar at the bottom shows an overview of general switch parameters and also the status of the configuration storage.

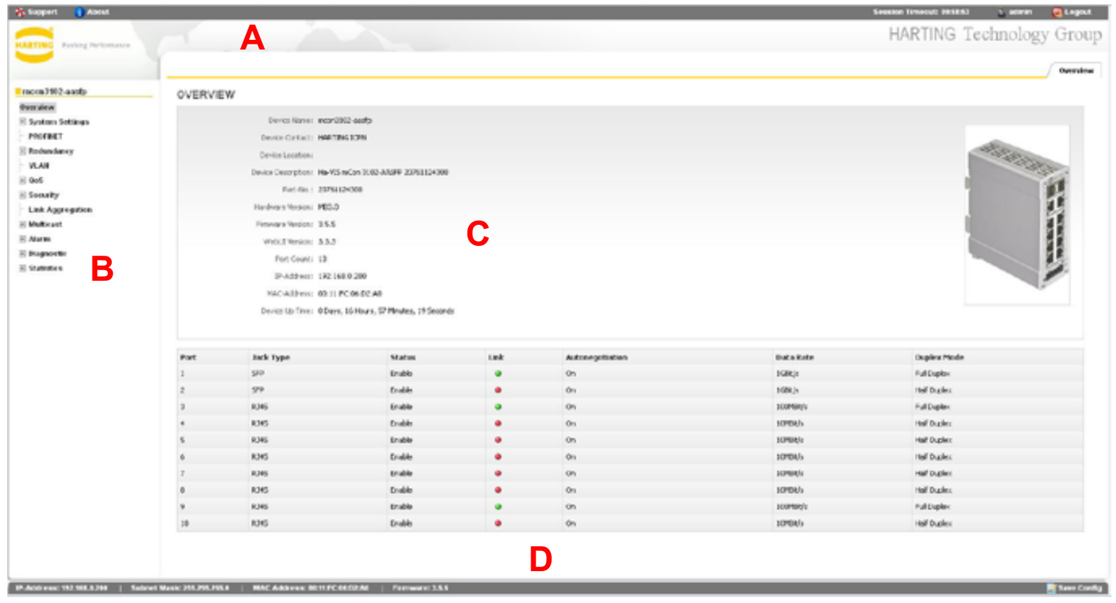


Figure 6-1 Screen structure

A The top task bar
B The menu tree
C The active window
D The bottom task bar

6.1.1 The top task bar

The task bar at the top of the window contains links to *Support*, *About* and *Logout*. It is necessary to use the logout button before closing the browser, to be sure that the web session is terminated correctly.

6.1.2 The menu tree

A clickable, two-level menu located on the left of the browser window is used to navigate through the switch functionality. You can view or change switch settings and statistics by clicking on any of the various second-level menu choices.

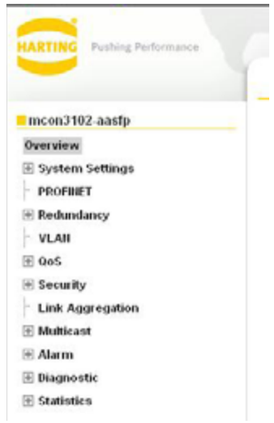


Figure 6-2 The menu tree

6.1.3 The active window

Most of the screen is taken up with the active window, in which settings and statistics for the switch are displayed and configured. The active window consists of several tabbed sub-windows. The right-most tabbed section is marked with a question mark and contains helpful explanations for the corresponding settings.

6.1.4 The bottom task bar

On the left side the IP Address, the Subnet Mask, the MAC Address and the installed firmware version of the switch is displayed. On the right side, the current configuration storage status is shown.

6.2 Accept and saving changes with the Save Configuration button

After modifying a setting (e.g. by checking a box or specifying a value), please click on the *Apply* button located at the bottom of the active window to confirm the change. Note that the *Apply* function only temporarily saves the changes to the RAM. For a short time after the opening of a window, the *Apply* button is highlighted grey. The *Apply* button is also activated, when settings or alterations are made in the window. In this case, it appears in a bold font to remind you that settings have been made or altered and that these have to be confirmed by clicking the *Apply* button. After this is done, a *SAVE CONFIGURATION* button appears in the bottom bar. Click the button to save your changes permanently in the flash memory to make the configuration also existent after a power down or a software reboot.

Figure 6-3 Save Configuration button

Assuming configuration changes and permanently saving them

- The software maintains any configuration changes in volatile memory after pressing the *Apply* button.
- The administrator must explicitly trigger the save operation (bottom bar after changing parameters.
- When triggered, the software saves the full configuration.
- Any old contents in the config-file is over-written.
- When the switch is restarted, the software starts with the last configuration saved to the flash.

Note

The *Apply* button only saves your changes temporarily until the next reboot. You have to click on the subsequent *SAVE CONFIGURATION* button in order to save the changes persistently.

6.3

If you specify an invalid entry (for example, an out-of-range timer value or improperly formatted IP address), a red exclamation mark is displayed next to the error field to notify the user of the error.

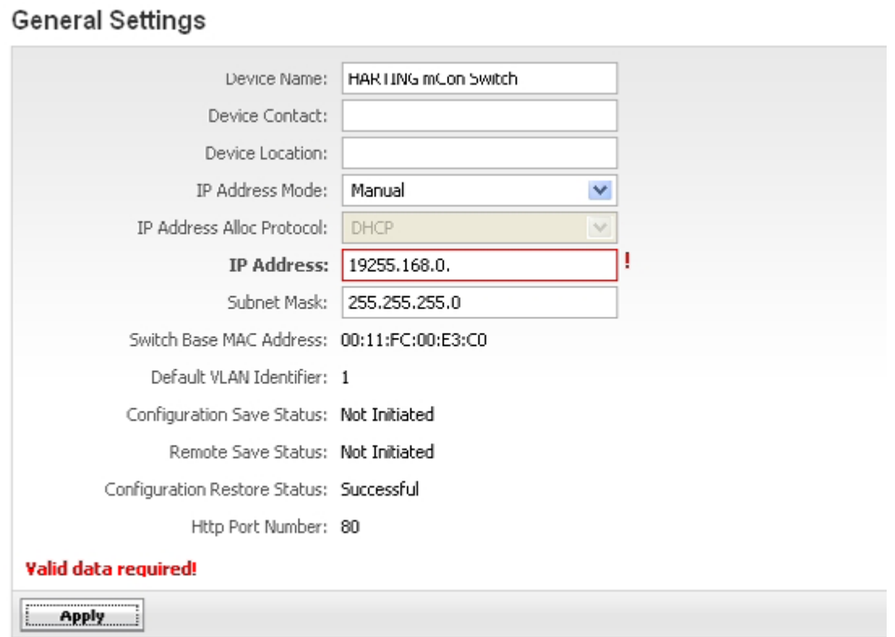


Figure 6-4 Invalid entry: The exclamation point indicates an improperly formatted IP address.

6.4 User rights

There are two pre-defined user modes for accessing the Ethernet switch web-based software:

Function	Description
Guest	The access category *Guest* enables all areas of the software to be viewed only.
Admin	The access category *Admin* enables all areas of the software to be viewed and administered. No restrictions apply to making settings or alterations. This is the normal administrative user account for making switch settings.

7. Overview

After you log in to the switch, the active window displays an overview of the switch and the main settings for each of the ports. No changes can be made in this window. To access this section, simply click on *Overview* in the two-level menu tree displayed at the left of the window.

The top right section of the Overview window contains an illustration of the particular Ethernet switch you are connected to. In addition, general information is displayed at the top left of the Overview window:

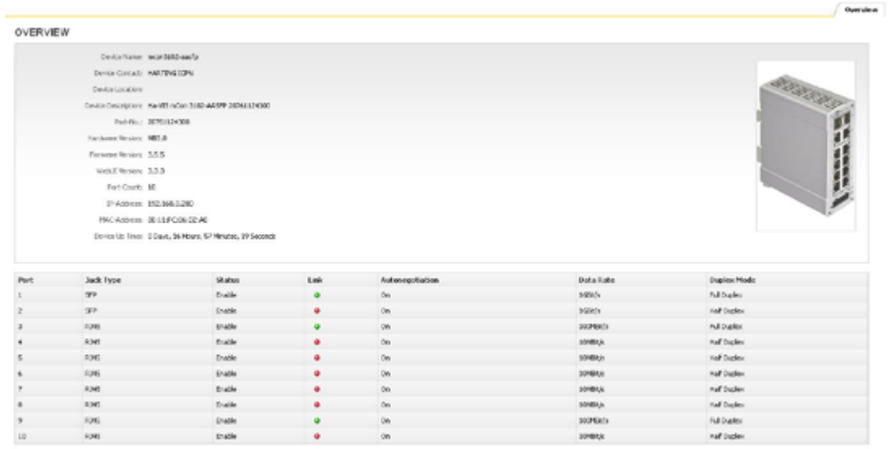


Figure 7-1 The Overview section

Function	Description
Device Name	Displays the type of HARTING Ethernet switch in use. **Default value:** *Ha-VIS mCon 3080-A, Ha-VIS mCon 3102-AASFP*
Device Contact	Displays contact information, as defined by the user in the **General Settings** section.
Device Location	Displays the location of the device, as defined by the user in the **General Settings** section.
Device Description	MAC address of the switch
Part No.	Displays the HARTING part number of the switch.
Hardware Version	Displays the hardware version number of the switch management board.
Firmware Version	Displays the firmware version number of the switch.
WebUI Version	Displays the version of the web interface.
Port Count	Displays the number of ports.
IP-Address	Displays the currently assigned IP address on the switch.
MAC-Address	Displays the unique hardware MAC address on the switch.
Device Up Time	Displays the duration that the switch has been powered up.

The table at the bottom of the Overview window has the following columns for each port (see table below).

Note

It is impossible to change information in the Overview window. Basic port settings can be altered from the *System Settings → Port Settings* menu section.

Function	Description
Port	Displays all available switch ports.
Jack Type	Displays the compatible media or jack type for the port (*RJ45*, or *SFP*).
Status	Displays the current status of the port. *Enable* means that the port is enabled; *Disable* is displayed if the port is disabled. (A port can be disabled in the *System Settings → Port Settings* section.)
Link	Displays the status of the port. A red circle indicates that there is currently no existing link, while a green circle indicates an existing link.
Auto Neg	Displays the negotiation state. Auto-negotiation is a technology for ensuring compatibility of a network component with the network. This column indicates if the Auto-negotiation function for the port is activated (**ON**) or deactivated (**OFF**).
Data Rate	Displays the data transfer mode for the respective port.
Duplex mode	Displays the port duplex mode. *Half duplex* means that data flows in one direction via the port at a given time; *Full duplex* enables data flow in both directions.

8. System Settings

The System Settings section is composed of the following sub-sections: *General Settings*, *Port Settings*, *User Management*, *SNMP*, *Network Discovery*, *Time Settings*, *DHCP Relay Agent* and *File Transfer*. All of this sections are described below.

8.1 General Settings and Switch Management

8.1.1 General Settings

In order to commission the Ethernet switch, the IP address and subnet mask must first be modified for the connected network (refer to the *Quick-start Guide* for setup instructions). If a DHCP server (Dynamic Host Configuration Protocol) is running on your LAN, you can specify *Dynamic* in the *IP Address Mode* settings.

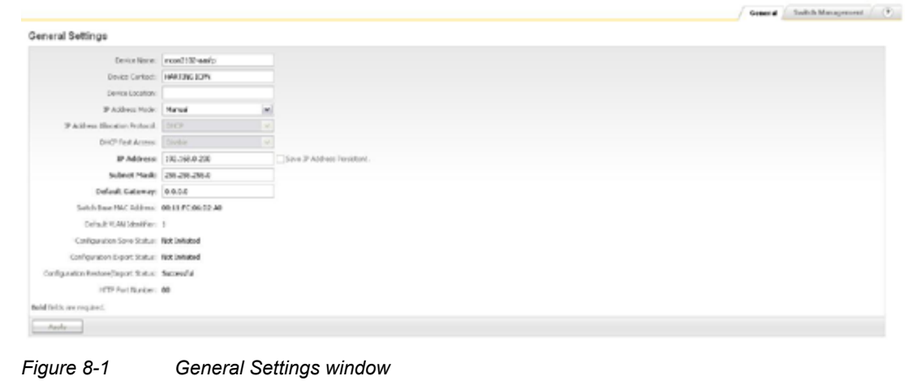


Figure 8-1 General Settings window

The following general settings can be displayed or specified:

Function	Description
Device Name	Specify a descriptive text for the device name.
Device Contact	Specify a descriptive text for the device contact.
Device Location	Specify a descriptive text for the device location.
IP Address Mode	Specify the switch IP addressing mode. If *Dynamic* is selected in the drop-down list, the switch is assigned with a valid IP address and subnet mask during system initialisation by the DHCP server. If *Manual* is selected, the IP address and the subnet mask must be entered manually.
DHCP Fast Access	The function accelerates the DHCP addressing in large networks. The standard timeouts and waiting periods are reduced to a minimum. It is recommended to set this option to *enable*, if Option 82 is used.
IP Address	Specify the IP address of the switch. IP addresses are assigned automatically if a DHCP server is activated.

Note

The IP address assigned to the switch must be **unique** for the respective network! Connectivity problems will arise if two network components are assigned the same IP address.

Function	Description
Save IP Address Persistent	Check this box to save the IP address permanently. You will no longer be able to connect to the switch using the old IP address. Using your web browser, connect to the switch using the new IP address.
Subnet Mask	Specify the subnet mask for the network. If the subnet mask is entered manually. This value is assigned automatically if you have a DHCP server.
Default Gateway	Specify the default gateway for the switch

Be sure to remember to click on the *Apply* button to save your changes. Then click on the *Save Configuration* button which appears at the bottom of the window to save the settings permanently.

The lower section of the *General Settings* window lists additional status information. This includes: the switch MAC address, the default VLAN identifier, the configuration save status, the remote save status, the configuration restore status and the HTTP port number.

8.1.2 Switch Management

This chapter describes the configuration of the various system and session related features, like web session and service functionalities.

Figure 8-2 Switch Management window

Web Session

Function	Description
Web Session Timeout	Sets the timeout for each web session. Without any action on the web interface, the session will be terminated after the timeout timer expires. **Range of value:** 1 ... 3600 seconds **Default value:** 600
Maximum Number of Web Sessions	Sets the maximum number of parallel web sessions. **Range of value:** 1 ... 10 **Default value:** 2

Management

Function	Description
Default/Mgmt-VLAN ID:	Change of the Management VLAN **Range of value:** 1 ... 4094 **Default value:** 1
HTTP Port	Sets the http port for the web interface. **Range of value:** 1 ... 65535 **Default value:** 80
Multifunction Button	Enable or disable the Multifunction Button on the switch **Range of value:** *Enable* / *Disable* **Default value:** *Enable*

8.2 Port Settings

This section informs you on how to change the settings for the switch's Ethernet ports. The ports can be individually enabled (up) or disabled (down). The data transfer rate and mode of data flow can be determined as well as the compatibility parameters for the network. Note that there are two tabbed sections (*Basic Settings* and *Port Control*) where these settings can be made.

8.2.1 Basic Settings

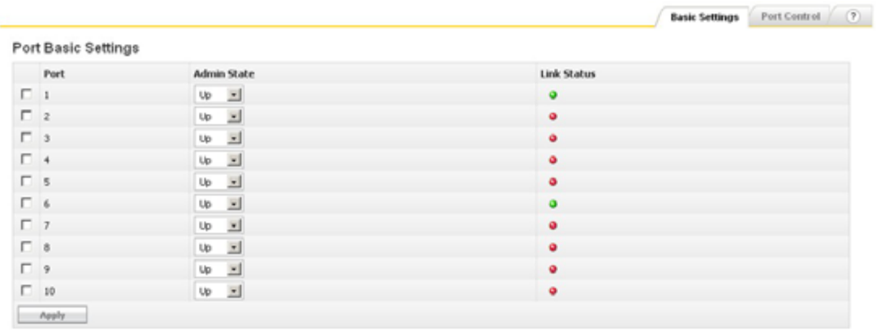


Figure 8-3 Basic Settings tab

In this tabbed section, the administrative state of individual ports can be specified. Each port row has the following columns.

Function	Description
Select/Port	Select the port that you would like to change by clicking on the checkbox here.
Admin State	Select the desired state of the port. A port can be either enabled (up) or disabled (down). **Range of value:** *UP* / *DOWN* **Default value:** *UP*
Link Status	Displays the port status. A green circle in this column indicates that a device is connected to this port. A red circle indicates that no device is connected.

8.2.2 Port Control

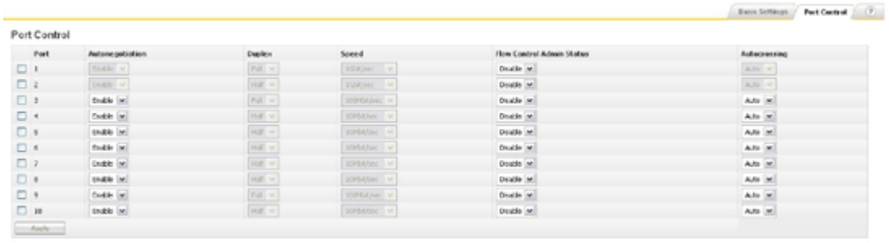


Figure 8-4 Port Control tab

In this tabbed section, the characteristics of individual ports can be specified in the following columns:

Function	Description
Select/Port	Select the port that you would like to change by clicking on the checkbox here.
Autonegotiation	Select whether Autonegotiation is disabled or enabled. Autonegotiation is a function which enables the participating interfaces to automatically determine the best possible transmission parameters. The auto-negotiation function can either be activated (*Enable*) or deactivated (*Disable*). If *Enable* is selected, the auto-negotiated settings will be used and the data-rate and duplex columns will be greyed out. **Range of value:** *Enable* / *Disable* **Default value:** *Enable*
Duplex	Select the data transmission mode for the respective port from the drop-down list. *Half* means that data flows in only one direction via the port at a given time; *Full* enables data to flow in both directions simultaneously. **Range of value:** *Half* / *Full* **Default value:** *Full*
Speed	Select the data transmission rates for the port from the drop-down list: 100 Mbit/s or 10 Mbit/s, 100 Mbit/s or 1 Gbit/s, depending on the type of port interface. **Range of value:** *10 Mbit/s* or *100 Mbit/s* / *100 Mbit/s* or *1 Gbit/s* **Default value:** Physical maximum
Flow Control Admin Status	Select if flow control is activated (*Enable*) or deactivated (*Disable*). If enabled, the port sends out Pause frames when the buffer capacity reaches a certain limit. **Range of value:** *Enable* / *Disable* **Default value:** *Disable*
Autocrossing	The automatic crossover of the RX / TX lines can be switched from the standard auto mode in the following modes: MDI (no crossing of lines), MDIX (RX / TX lines are crossed) and AUTO (automatic crossover). **Range of value:** *MDI* / *MDIX* / *AUTO* **Default value:** *AUTO*

Note

For the usage of the Ha-VIS mCon 3102-AASFP the following restrictions apply: Depending on the capabilities of the used SFP-modules the adjustable parameters may vary. For example, it is not possible to deactivate Autonegotiation and Autocrossing for Gigabit SFP-Modules.

8.3 User Management

This section allows you to create new users and to specify a new password for the *admin* or *guest* account.

8.3.1 User Management

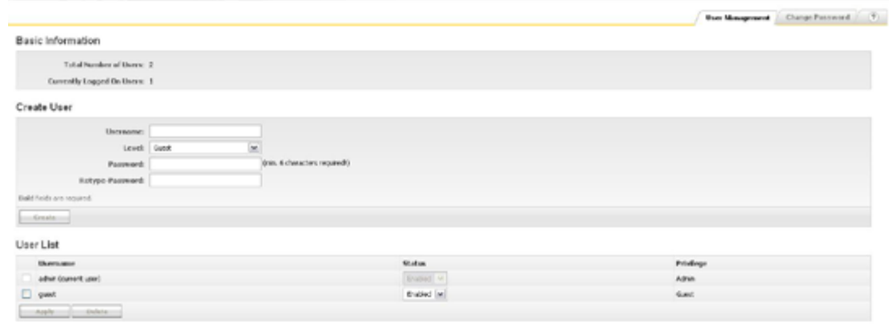


Figure 8-5 User Management tab

Create User

To create a new user you must be logged in to the switch as an administrator. It is possible to create new *Guest* and *Admin* accounts. After the required information has been entered, the *Apply* button must be pressed and finally the creation of the new account must be verified with the password of the actual logged in user account.

User List

All users existing on the switch are shown in this list. The maximum of users is limited to 20. Selected users can be deleted from the switch by pressing the delete button on the bottom. The default admin account can only be deactivated, if another admin account was created on the switch first. You must be logged in via this new admin account to deactivate the *Default Admin* account.

8.3.2 Change Password

Figure 8-6 Change Password tab

The switch software is password-protected to prevent unauthorized access. The admin password should consist of at least six characters. The password must always be entered to gain access to the software.

There are two access levels, which can be chosen from the drop-down list:

Function	Description
Admin	All rights are available.
Guest	All settings and values can only be viewed. It is not possible to alter the password or other settings.

The system administrator is authorized to alter the valid password for the access levels for the administrator and guest in this section. The admin password must be specified correctly before you can change a password. Click *Apply* to confirm your entry. The new password will become valid when the switch is rebooted.

If the administrator password is forgotten or if it becomes necessary to alter it due to technical reasons, this process can be carried out using the Multifunction Button. To learn how to use the Multifunction Button refer to Chapter 5 – **„Multifunction Button“**.

8.4 SNMP

SNMP (Simple Network Management Protocol) is the most widely-used network management protocol on TCP/IP-based networks. SNMP provides an easy mechanism for managing a network using a simple Command-Response protocol defined between the Manager and the managed entities. The management is performed through MIBs (Management Information Base) supported by the managed entities. The MIBs contain configuration elements which can be either Viewed (GET) or Modified (SET) by the Managers.

SNMPv3 is designed mainly to overcome the security shortcomings of SNMPv1/v2. USM (User based Security Model) is the main feature added as part of the SNMPv3 specification. USM provides for both encryption and authentication of the SNMP PDUs. With SNMPv3, the SNMP communication is completely safe and secure.

The configuration of the switch can be accessed and changed directly using SNMP commands. This section allows you to specify the basic SNMP settings. This switch software supports SNMP versions 1/2c and 3. You may also enable both versions simultaneously.

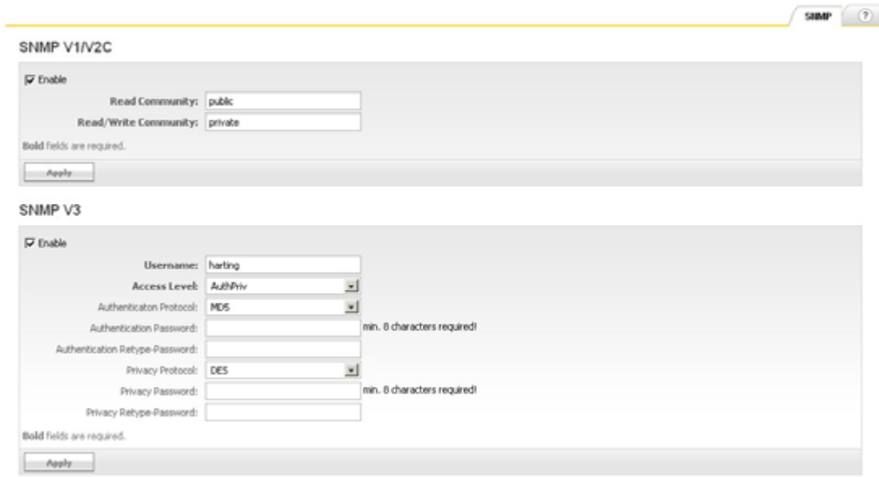


Figure 8-7 SNMP section

8.4.1 SNMP V1/V2C

For V1/V2 operations, the HARTING SNMP Agent provides a community-based *Security Mechanism*. *Community* names are encoded into V1/V2 messages and the Agent verifies the privilege status of the community name before responding to it. Community names are associated with the privilege status. The privilege status can be of the types read-only or read-write.

Function	Description
Enable	Check this box to launch the SNMP agent and allow access to the switch via SNMP version 1/2c. **Range of value:** *Enable* / *Disable* **Default value:** *Enable*
Read Community	Specify the community name for SNMP read access. The default is *public*. **Range of value:** Not more than 20 printable characters. **Default value:** *public*
Read/Write Community	Specify the community name for SNMP read and write access. The default is *private*. This community string acts as an SNMP password; you should pick one that it difficult to guess. **Range of value:** Not more than 20 printable characters **Default value:** *private*

8.4.2 SNMP V3

The HARTING SNMP Agent provides complete support for User based Security Model.

The following security algorithms are supported:

- **Authentication** HMAC MD5 and HMAC- SHA
- **Encryption** DES-CBC

Three levels of security are supported.

- **NoAuthNoPriv** No Authentication and no Privacy
- **AuthNoPriv** Authentication and no Privacy
- **AuthPriv** Authentication and Privacy

Function	Description
Enable	Check this box to launch the SNMP agent and allow access to the switch via SNMP version 3. **Range of value:** *Enable* / *Disable* **Default value:** *Enable*
User	Specify the user name for SNMP version 3 access. **Range of value:** Not more than 20 printable characters. **Default value:** *harting*
Access Level	*NoAuthNoPriv* No authentication and no message encryption *AuthNoPriv* Enables message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication, but no message encryption *AuthPriv* Both authentication and message encryption. **Range of value:** *NoAuthNoPriv* / *AuthNoPriv* / *AuthPriv* **Default value:** *AuthPriv*

Function	Description
Authentication Protocol	Protocol used for User Authentication (MD5) or Secure Hash Algorithm (SHA) **Range of value:** *MD5* / *SHA* **Default value:** *MD5*
Authentication	Specify the SNMPv3 password. It must be at least eight characters. **Range of value:** Not more than 20 printable characters **Default value:** none
Authentication Retype Password	Repeat the specified SNMPv3 password.
Privacy Protocol	Protocol used for privacy. **Range of value:** *DES* **Default value:** *DES*
Privacy Password	Specify the SNMPv3 privacy password. **Range of value:** Not more than 20 printable characters **Default value:** none
Privacy Retype Password	Repeat the specified SNMPv3 privacy password.

Note

If you don't plan to use SNMP, you should make sure that both versions are disabled so that maximum security is ensured.

Note

A MIB (Management Information Base) file can be found on the enclosed CD. With the MIB information you get open-standard access to the switch using SNMP management software.

8.5 Network Discovery

This section allows you to activate and configure LLDP (Link Layer Discovery Protocol). LLDP can be used to determine the capabilities of devices on your network. It allows the switch to announce its capabilities and other media-specific configuration information to the local area network.

The LLDP allows systems on an Ethernet LAN to advertise their key capabilities and to learn about the key capabilities of other systems on the same Ethernet LAN. Consequently, this promotes a unified network management view of the LAN topology and connectivity to support network administration and trouble-shooting. The station and capabilities information is conveyed in protocol frames called Link Layer Discovery Protocol Data Units (LLD PDUs). In general, a network administration station can be connected to one single switch getting access from there to the connectivity information of the complete network within an enterprise. The switch also provides notifications in form of SNMP traps to alert the operator about changes in the network topology.

8.5.1 LLDP Settings

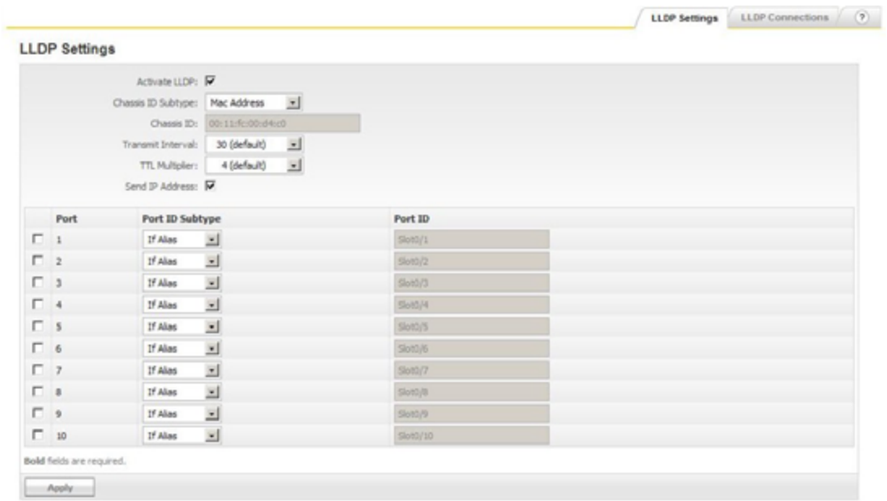


Figure 8-8 LLDP Settings tab (Network Discovery section)

The Refresh button at the bottom of this window allows you to refresh your view of neighbouring chassis IDs, port IDs, and IP addresses.

Function	Description
Activate LLDP	Select whether to disable or enable LLDP globally on the switch. **Range of value:** *Enable* / *Disable* **Default value:** *Disable*
Chassis ID Subtype	Select the Chassis ID Subtype which should be included in the LLDP packets. **Range of value:** *MAC Address* / *Interface Alias* / *Network Address* / *Custom* **Default value:** *MAC Address*
Chassis ID	Select the Chassis ID which should be included in the LLDP packets.
Transmit Interval	The interval at which LLDP frames are transmitted on behalf of this LLDP agent. The default value for the Transmit Interval is *30 seconds*. **Range of value:** *5, 10, 30, 60, 120 sec* **Default value:** *30 sec*
TTL Multiplier	Time-to-live value expressed as a multiple of the Transmit Interval **Range of value:** *2, 3, 4, 5, 10* **Default value:** *4*
Send IP Address	Option to transmit switch's IP adress with every LLDP packet **Range of value:** *Enable* / *Disable* **Default value:** *Disable*
Table description	Via the table, the Port ID can be set for each port individually.

Note

The interval between to LLDP PDUs is calculated using the following algorithm:
LLDP Interval = Transmit Interval x TTL Multiplier

8.5.2 LLDP Connections

Figure 8-9 LLDP Connections (Network Discovery section)

The LLDP Connections table shows all directly connected neighbours and the corresponding information. The *Refresh* button allows you to refresh your view of neighbouring chassis IDs, port IDs, and IP addresses. The following information are shown:

- **Local Port** Local port where the information was learned
- **Neighbour Chassis ID** Chassis ID of the neighbour device
- **Neighbour Port ID** Port ID of the neighbour device
- **Neighbour IP** IP address of the neighbour device

8.5.3 Advanced LLDP Settings

Figure 8-10 Advanced LLDP Settings (Network Discovery section)

In this menu, you can make more extensive settings for LLDP. You can enable or disable LLDP for a specific port. Select Tx only if you want to transmit LLDP-frames but don't want to receive LLDP-frames. Choosing Rx only causes that LLDP-frames can be received but not be transmitted. By default, both options are activated.

Function	Description
Port Config	Select this function if you want to send and/or receive LLDP frames on a specific port. **Range of value:** *Tx only* / *Rx only* / *Tx and Rx* / *Disable* **Default value:** *Tx and Rx*

8.6 Time Settings

This section allows you to set the system time for the switch. The time can be specified manually or automatically via an SNTP (Simple Network Time Protocol) server.

The Simple Network Time Protocol is a subset of the Network Time Protocol used to synchronize computer clocks in the Internet. HARTING switches implement the client portion of the SNTP protocol and do not implement the server portion. The administrator has the choice whether to set the system clock manually or to enable SNTP. If SNTP is enabled, the SNTP client gets the time from the server. The SNTP client also has callouts to set the system time based on the time received from the SNTP server.

8.6.1 Time Settings

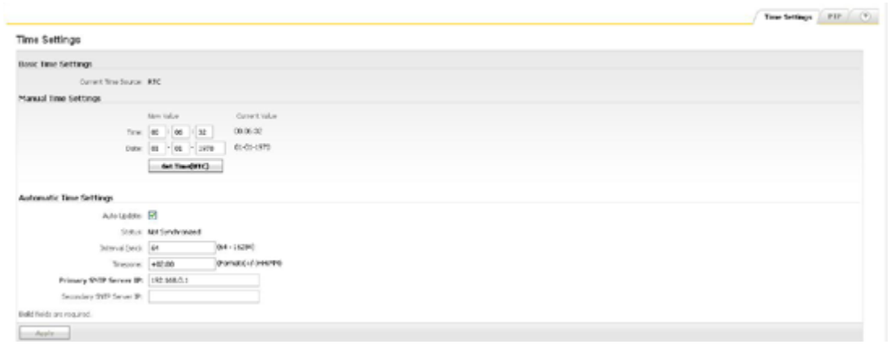


Figure 8-11 Time Settings window

Manual Time settings

Function	Description
Current Time Source	RTC/PTP/NTP
Time	Specify the system time manually. The current system time is displayed below *Current Value* in the format hours:minutes:seconds (24-hour format). The time can be specified manually in the *New Value* column.
Date	Specify the date manually. The currently set date is displayed below *Current Value* in the format day-month-year. The date can be specified manually in the *New Value* column.
Get Time	Click on this button to enter the computer system's time and date into the fields above. The time information will be taken from the computer on which the web browser is running.

Automatic Time settings

Function	Description
Auto Update	Check this box in order to receive the system time automatically with the support of a SNTP server.
Status	Shows the current synchronization status
Interval	Specify the period of time in minutes. The system time is then updated periodically at this interval. **Range of value:** *64 - 16284* **Default value:** *64*
Time Zone	Specify the Time Zone **-12:00** ... **+ 12:00**
SNTP Servers	Specify the address of the SNTP servers that will supply the system time. The address can be that of either a publicly-accessible PC or a specified PC in the network that serves as a time generator. The IP address must be specified. More than one server may be specified to provide redundancy.

Note

The Ethernet switch stores time and date up to 72 hours after power off. By default, the switch starts with the following system settings after booting up:

Time 00:00:01

Date 01-01-1970

The Ethernet switch does not automatically adjust to summer and winter time. This should be taken into account when evaluating log files or alarm-generated e-mails in which the time is logged.

8.6.2 Precision Time Protocol (PTP)

PTP, in accordance with standard 1588v2, is a network protocol to synchronize the time of multiple participants in a network. A PTP network consists of a hierarchical structure made up of clocks which are synchronized with each other. One of the clocks is the "grandmaster clock" with which all the other clocks are synchronized. Which participant is considered the "grandmaster clock" is determined using the "best master clock" algorithm.

HARTING Ha-VIS mCon 3000 switches can be operated in the following PTP modes:

- **Boundary Clock:** The device can either be a master or a slave. As a slave, the switch synchronizes the clock with another master. The master itself provides its time to the other slaves.
- **End to End transparent clock:** The switch forwards the PTP messages which are exchanged between the masters and the slaves and adds the processing time in the switch itself to the correction field in the message. The slaves can use this to determine the correct time.
- **Peer to peer transparent clock:** The switch forwards the PTP messages which are exchanged between the masters and the slaves and adds the processing time in the switch itself and the link delay to the correction field in the message. The slaves can use this to determine the correct time.

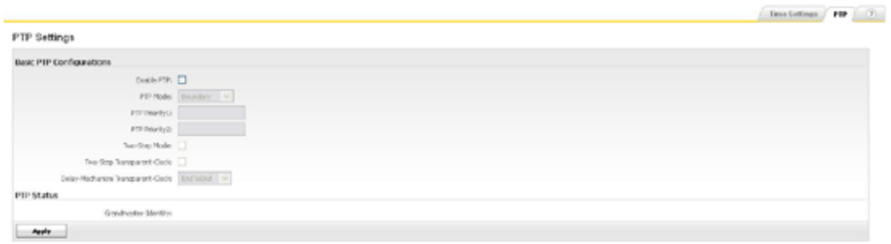


Figure 8-12 PTP Settings section

The following settings can be made in this menu:

Function	Description
Enable PTP	Switch PTP on or off
PTP Mode	Selection of the operating mode **Range of value:** *Boundary / Transparent*
PTP Priority 1	Enter the priority 1. Available only in boundary mode **Range of value:** *0...255* **Default value:** *0*
PTP Priority 2	Enter the priority 2. Available only in boundary mode **Range of value:** *0...255* **Default value:** *0*
Two-Step Mode	Define whether the switch device should send only Sync-Messages or whether it should send Sync Messages and FollowUp Messages, which means Two-Step-Clock. (Boundary mode only)
Two-Step Transparent-Clock	Define whether the switch device should send only Sync-Messages or whether it should send Sync Messages and FollowUp Messages, which means Two-Step-Clock. If the device receives Sync Messages from a one Step Device, it will generate the FollowUp Messages. (Transparent mode only)
Delay-Mechanism Transparent-Clock	Specify the delay mechanism of the transparent clock. (Transparent mode only) **Range of value:** *End to End / Peer to Peer*

8.7 DHCP Relay Agent

Upgrading and changing the structure of Ethernet networks usually causes a lot of administrative effort. Configuration of security and addressing procedures has to be redone every time a device is replaced. Replacing or moving network devices often causes a lot of trouble, because some network mechanisms such as dynamic IP address assignment are MAC based.

DHCP Option 82 provides a mechanism for generating IP addresses based on the location of the client device in the network. A client device can be any device attached to the switch or the switch itself.

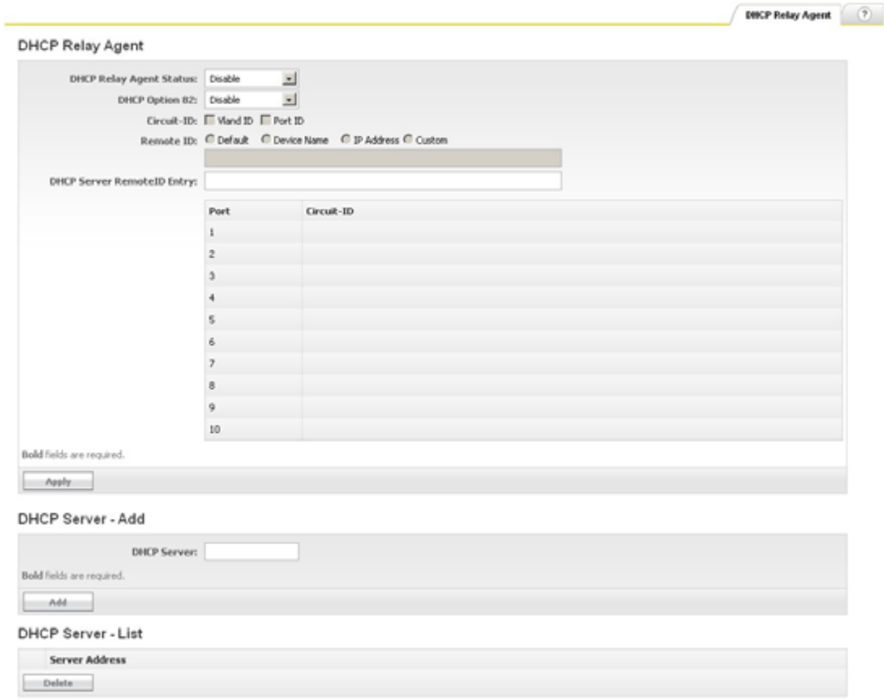


Figure 8-13 DHCP Relay Agent tab

Function	Description
DHCP Relay Agent Status	Enables or disables the DHCP Relay Agent on the switch. To use Option 82 this option must set to enable. **Range of value:** *Enable / Disable / Enable RFC conform* **Default value:** *Disable*
DHCP Option 82	Select whether to disable or enable Option 82 on the switch. **Range of value:** *Enable / Disable* **Default value:** *Disable*
Circuit-ID	Defines the Circuit-ID to identify the location of the end device in the network. **Range of value:** *VLAN ID / Port ID*

Attention:

The Port ID must be checked to guarantee the correct work of DHCP Option 82.

Function	Description
Remote ID	Defines the Remote-ID for the switch which will be added to the DHCP packets. *Default* Set the Remote-ID to the default value (MAC address). *Device Name* Add the Device Name as Remote ID. *Custom* A custom value can be added as the Remote-ID.
DHCP Server RemoteID Entry	Enter calculated value of the Remote ID. If the Remote ID is used by the DHCP Server, this value must be entered on the server side.
DHCP Server	The IP address of the DHCP Server must be entered.
DHCP Server List	Shows a list of all configured DHCP Server.

8.8 File Transfer

This section allows you to transfer files to and from the switch. File transfers are used for importing or exporting specific saved configurations and for importing or exporting firmware. Uploading and downloading of the files can be done via a TFTP Server and very simple via HTTP.

The address of a TFTP (Trivial File Transfer Protocol) server can be specified for importing or exporting firmware or configurations. In order to transfer files to or from the switch, a TFTP server program must be installed on a connected PC. There are three different tabbed sections within this window.

8.8.1 Firmware

This tabbed section allows you to specify the IP address of the TFTP (Trivial File Transfer Protocol) server and the file name of the firmware file to be exported or imported.

Be sure that you have the TFTP server running and configured properly on a separate computer. Click on the *Import* or *Export* button to begin the transfer.

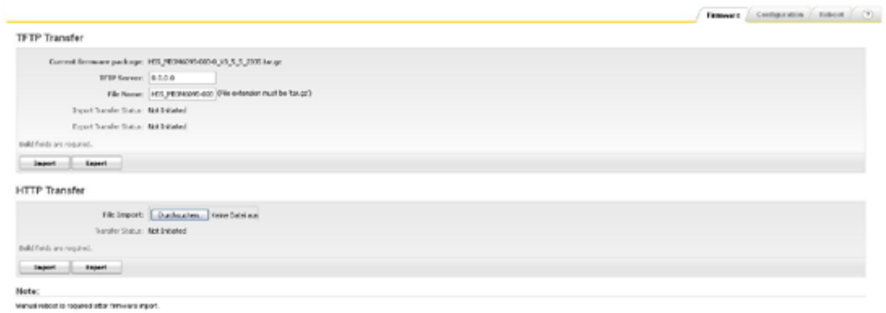


Figure 8-14 Import/Export Firmware tab

Import (Load) a firmware

Select *Import firmware* in order to import a specified firmware file.

Select *Import* to import the current firmware from the TFTP server or via HTTP from a remote file system. This option is used to do a firmware update of the switch.

Export (Save) a firmware

Save the current firmware to a file on a remote system.

Select *Export* to export the current firmware to the TFTP server or via HTTP to a remote file system.

TFTP Transfer

This section allows you to specify the IP address of the TFTP (Trivial File Transfer Protocol) server and the file name of the firmware file to be exported or imported.

Be sure that you have the TFTP server running and configured properly on a separate computer.

Function	Description
TFTP Server	Specify the IP address of the TFTP server
File Name	Specify the file name of the configuration

Click on the *Import* or *Export* button to begin the transfer.

Note

The transfer status is shown in this window and will be updated automatically. Also check in your TFTP server logs to see when the transfer is complete. Wait until the TFTP server log shows that the file has been transferred and the status on the web interface shows successful before rebooting.

If you intend to load a new version of the firmware file from the TFTP server, we recommend first of all to back up the existing firmware file to the TFTP server. Please note that the switch only accepts a correct und successful uploaded firmware file for updating the software. A wrong file or a abortion during the upload will not cause any damage or inoperability of the switch.

HTTP Transfer

This section allows you to use HTTP data transfer for the firmware file to be exported or imported.

Click on the *Import* or *Export* button to begin the transfer.

To import a new firmware file, just click on the browse button to search for a file on a remote system and select it via the standard windows interface. After the selection of the file, click to *Import* to start the upload of the firmware.

To export the current firmware of the switch, click on the *Export* button and the standard windows interface will enable you to save the file to a remote system.

ATTENTION

Only select firmware files that are compatible with the device for the import functionality.

8.8.2 Configuration

This tabbed section allows you to load or save a configuration. The following settings are available.

Figure 8-15 Save/Load Configuration tab

Load Type

Function	Description	
Load Type	*Load Config on Startup*	Startup with the last saved configuration
	Load Factory default on Startup	Startup with factory defaults

The status of the current action is shown at the bottom of the box.

To start the switch with the factory default settings, you have to select *Load Factory default on Startup*, press the *Apply* button and restart the switch.

Import (Load) a configuration

Select *Import Configuration* in order to import a specified configuration file.

Select *Import Configuration* to import the current configuration from the TFTP server or via HTTP from a remote file system.

Export (Save) a configuration

Save the current configuration to a file on a remote system.

Select *Export Configuration* to export the current configuration to the TFTP server or via HTTP to a remote file system.

TFTP Transfer

Function	Description
File Name	Specify the file name to which the configuration file will be saved. **Default value:** *hss_config_files.cpak*
TFTP Server	Specify the IP address of the TFTP server where you will save the configuration.

The status of the current action is shown at the bottom of the box.

8.8.3 HTTP Transfer

This section allows you to use HTTP data transfer for the firmware file to be exported or imported.

Click on the *Import* or *Export* button to begin the transfer.

Note

Reboot is required after restore/import.

8.8.4 Reboot

To reboot the switch, click the Reboot button in this section.

A timer will wait 10 seconds before executing the reboot. This is helpful if large networks should be rebooted at the same time. The delay ensures that every switch in the network receives the command.

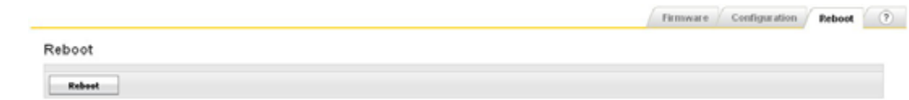


Figure 8-16 Reboot tab

9. PROFINET

In this section you learn how to activate the PROFINET IO Stack. By default it is not activated.

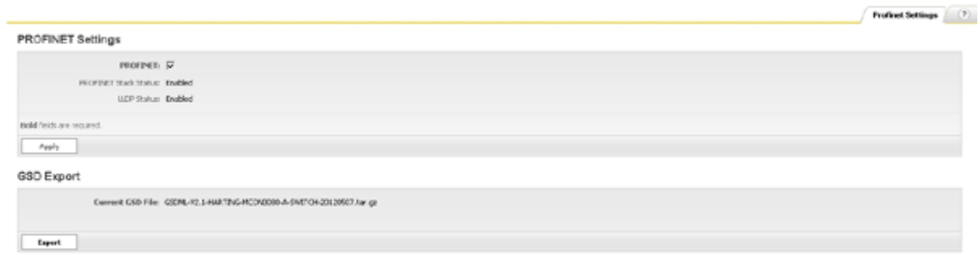


Figure 9-1 PROFINET window

If PROFINET is checked, the following settings are operated:

- LLDP will be activated (if it was disabled before).
- The PROFINET IO Stack will be enabled.

In the next window, you can choose between three options (see figure 9-2).

With GSD Export you can download the GSD file from the switch to a specified location via HTTP.

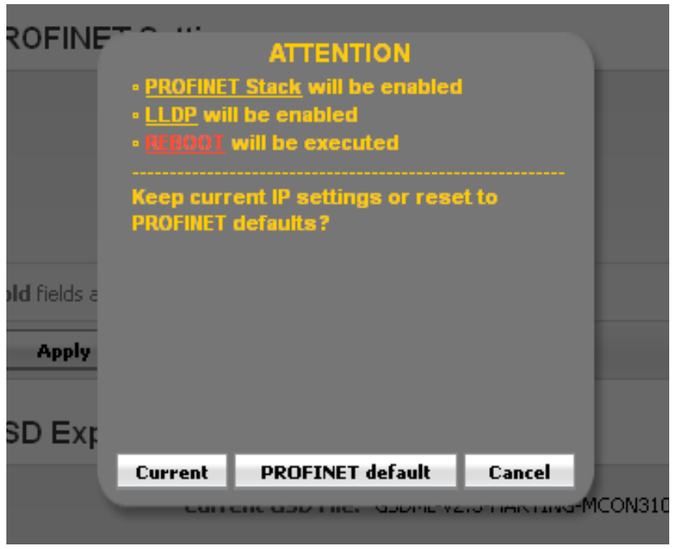


Figure 9-2 IP settings in PROFINET Profile

Choose the button “Cancel” to abort the task for enabling the PROFINET Profile.

Choose “Current” to enable “PROFINET” and keep the current IP Address settings.

Choose “PROFINET default” to enable PROFINET and use the Profinet default IP Address settings.

To be reachable via web interface, the switch needs to get a new IP address from the PROFINET controller.

Note

The switch will reboot automatically after enabling or disabling the IO Stack.

After a reboot, the diagnosis LED is flashing red/green until the switch and controller are successfully connected.

Note

All following configurations should be done by an engineering tool in the PROFINET environment!

Note

It is impossible to disable LLDP and to change the Transmit interval while checking PROFINET.

The following LLDP settings will automatically be made.

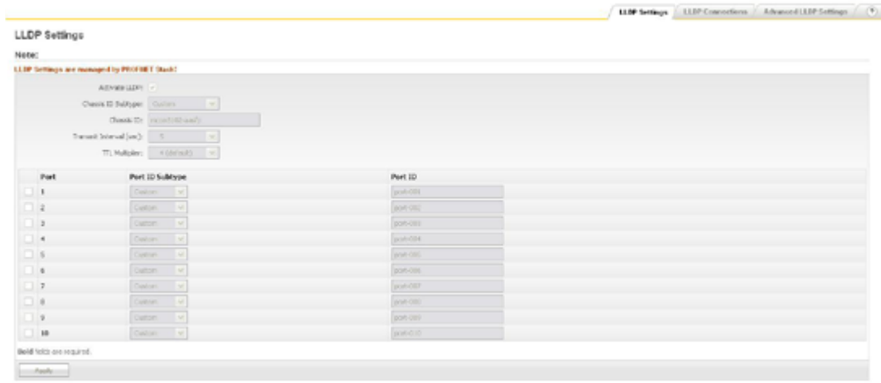


Figure 9-3 LLDP settings for PROFINET

10. Redundancy

10.1 RSTP

This section allows you to construct redundancy within your network topology. Redundant or spare links can be implemented to provide automatic backup paths if an active link fails.

STP (Spanning-Tree Protocol) is a link management protocol that provides path redundancy while preventing undesirable loops in the network that are created by multiple active paths between stations. To establish path redundancy, STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state. For an Ethernet network to function properly, only one active path must exist between two stations. Multiple active paths between stations in a bridged network can cause loops in which Ethernet frames can endlessly circulate. STP can logically break such loops and prevent looping traffic from clogging the network.

One of the problems with the Spanning Tree algorithm is that, in a large LAN, it can take a considerable time for the LAN topology to stabilize following a reconfiguration event - times of the order of 30 seconds being typical of the original form of the algorithm. To avoid this, HARTING supports RSTP (Rapid Spanning Tree Protocol). The operation of RSTP provides rapid recovery of connectivity in case of a link failure. RSTP avoids large delays by calculating an alternate root port and immediately switching over to the alternate port if the root port becomes unavailable RSTP in compliance with IEEE 802.1D (2004).

This section is divided into three tabbed sections for altering and viewing RSTP parameters: *Basic Settings*, *Port Settings* and *Port Status*. Each of these tabs is described below.

Note

When the switch boots up, RSTP is enabled by default. The default configuration is applicable for most applications, thus, usually no additional configurations have to be done in this section.

10.1.1 Basic Settings

Figure 10-1 Basic Settings tab

The tabbed section on p. 41 allows you to specify the following global settings.

Function	Description
Status	Select whether to disable or enable a global redundancy protocol on the switch. **Range of value:** *Enable* / *Disable* **Default value:** *Enable*
Version	Select the protocol version. **Range of value:** *RSTP Compatible* / *STP Compatible* **Default value:** *RSTP Compatible*
Priority	Specify the STP priority. This is used to identify the root bridge in a spanning tree. The bridge with the lowest value has the highest priority and is the root. A higher numerical value means a lower priority; thus, the highest priority is 0. The highest numerical value on the drop-down list is 61 440. **Range of value:** *0 ... 61 440* in steps of 4096 **Default value:** *32 768*
Max Age	Specify the time in seconds (STP) or hop count (RSTP) that the information received in a RSTP BPDU (bridge protocol data unit) is valid. **Range of value:** *6 ... 40* **Default value:** *20*
Hello Time	Specify the time interval in seconds between two successive configuration BPDUs. **Range of value:** *1 ... 2 sec* **Default value:** *2 sec*
Tx Hold Count	Specify the maximum number of BPDUs that can be transmitted in a second. **Range of value:** *1 ... 10* **Default value:** *6*
Forward Delay	Specify the period of time in seconds that a bridge will wait (the listen and learn period) before beginning to forward data packets. **Range of value:** *4 ... 30 sec* **Default value:** *15 sec*
Dynamic Path Cost Calculation	Select whether the dynamic path cost calculation is allowed or not. Cost calculation is allowed when this is set to *True*, the pathcost of all the ports will be calculated dynamically based on the speed of the interface. **Range of value:** *True* / *False* **Default value:** *True*

Note

It is recommended to use RSTP instead of STP to reduce the time for the network recovery in case of a link failure.

Note

The parameter *Max Age* must be set to the worst case diameter within a RSTP topology to prevent loops. In a ring structure of 20 switches for example, the *Max Age* value must be set to at least 20.

The following two mathematical relationships must be observed when assigning values for *Hello Time*, *Forward Delay* and *Max Age* parameters:

2 x (Forward Delay - 1) >= Max Age

Max Age >= 2 x (Hello Time + 1)

10.1.2 Port Settings

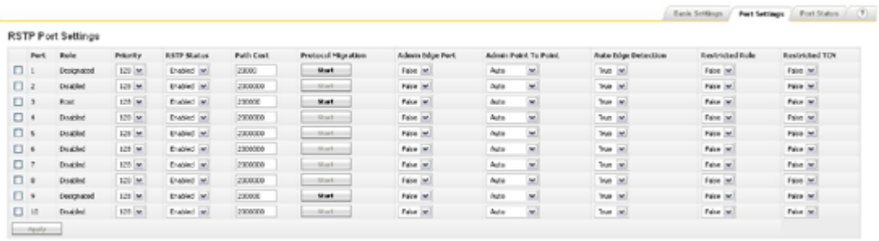


Figure 10-2 Port Settings tab

This tabbed section allows you to specify per-port STP settings. Changes can be made under the following columns:

Function	Description
Port	Select the port that you would like to change by clicking on the checkbox here.
Role	Displays the current role of the port. During the calculation of the spanning tree topology, each port is assigned a port role (root, designated, backup, alternate or disabled) based on how it will participate in the tree topology.
Priority	Specify the RSTP port priority. This is the value of the priority field located in the first octet of the port ID. **Range of value:** *0 ... 240* in steps of 16 **Default value:** *128*
RSTP Status	Select *Enabled* or *Disabled* to enable or disable RSTP for the corresponding port. **Range of value:** *Enable* / *Disable* **Default value:** *Enable*
Path Cost	Specify the path cost associated with this port. STP associates a path cost value to each port on each bridge. This value is an adjustable weighted measure that indicates the port's contribution to the route's transmission speed. Higher numerical costs indicate slower paths. 10 Mbit/s 2,000,000 100 Mbit/s 200,000 1 Gbit/s 20,000 **Range of value:** *0 ... 200,000,000*
Protocol Migration	When operating in RSTP mode, pressing the *Start*-Button forces this port to transmit RSTP BPDUs.
AdminEdge Port	Select *True* if the port is acting as an edge port. **Range of value:** *True* / *False* **Default value:** *False*
Admin Point to Point	Select the *Force True* option to configure a port as point-to-point. The port can be forced to a non-point-to-point state by selecting *Force False*. If you select *Auto*, the decision is made dynamically. **Range of value:** *Force True* / *Force False* / *Auto* **Default value:** *Auto*

Function	Description
Auto Edge Detection	Select *True* if you want to have the edge port status calculated dynamically. **Range of value:** *True* / *False* **Default value:** *True*
Restricted Role	Select the restricted role status of the port. If set to *True*, the port is restricted so that it may not be selected as a root port. A restricted port can be selected as an alternate port after the root port has been chosen. A *True* setting can result in poor connectivity within the spanning tree. **Range of value:** *True* / *False* **Default value:** *False*
Restricted TCN	Select the restricted TCN (Topology Change Notification) status of the port. If set to *True*, the port does not propagate received topology change notifications or topology changes to other ports. This prevents the topology change is caused by that port. **Range of value:** *True* / *False* **Default value:** *False*

10.1.3 Port Status

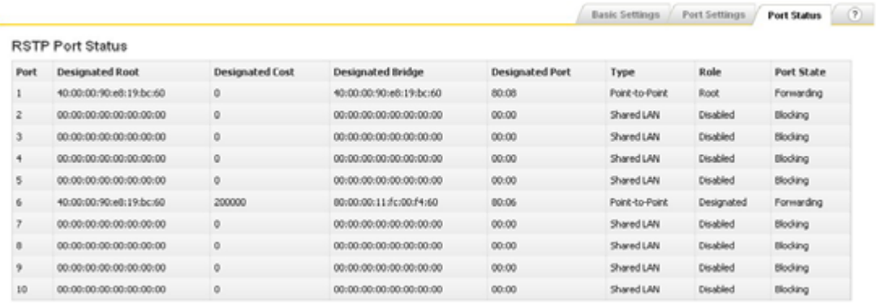


Figure 10-3 RSTP Port Status tab

This tabbed section allows you to view the status of each port; no settings can be specified or changed here. The following status information is shown:

Function	Description
Designated Root	Displays the unique bridge identifier (Priority + MAC address) of the bridge recorded as the root for the segment to which the port is attached.
Designated Cost	Displays the path cost of the designated port to the segment connected to this port.
Designated Bridge	Displays the designated bridge identifier (MAC address) of the bridge. This is the preferred bridge which this port considers as the designated bridge for its segment.
Designated Port	Displays the number of the port on the designated bridge for this port's segment.
Type	Displays the operation status of the LAN segment attached to this port. This indicates whether a port is considered to have a point-to-point connection or shared media.

Function	Description
Role	Displays the port's current role as defined by the Spanning Tree Protocol (root, designated, backup, alternate or disabled).
Port State	Displays the port's current state (*Forwarding*, *Blocking*, *Disabled* or *Learning*) as dynamically determined by STP.

10.2 MRP

The Media Redundancy Protocol (MRP) specifies a recovery protocol based on a ring topology. MRP is designed to react deterministically on a single failure. The MRP is implemented according to the IEC 62 439-2.

MRP memory cards allow you to activate the MRP functionality when using switches from the mCon Next Generation 3000 series. For example, in order to operate the device as an MRP slave, you need only have the corresponding MRP slave card inserted during operations.

If no valid SD card is plugged in, the following error message occurs:

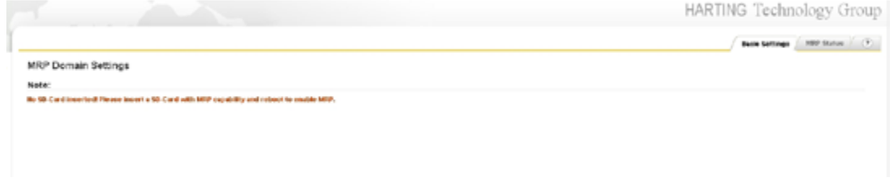


Figure 10-4 MRP Domain Settings with invalid SD card

With a valid SD card following page appears:

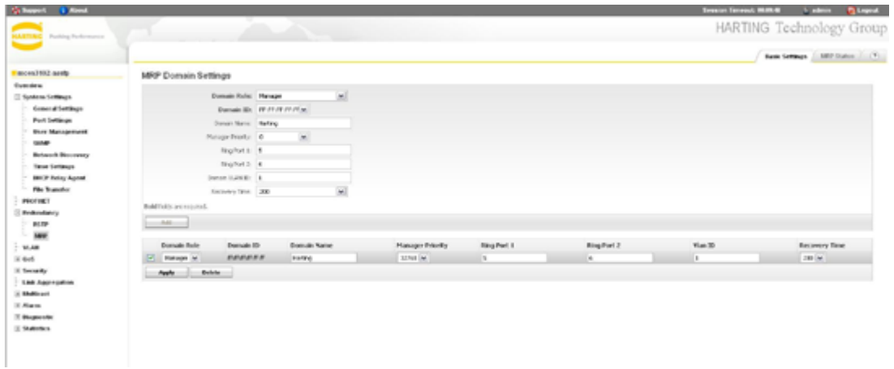


Figure 10-5 MRP Domain settings with a valid SD card

10.2.1 Basic Settings

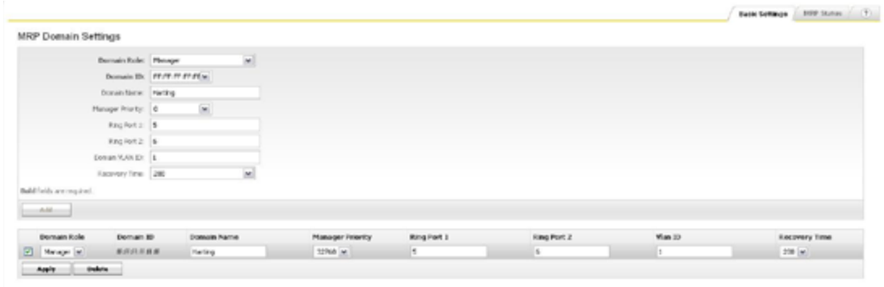


Figure 10-6 MRP Domain − Basic Settings

The following basical settings can be made:

Function	Description
Domain Role	Client or Manager depends on the inserted SD card
Domain ID's	4 UUID (Domain ID's) can be selected: **00:11:FC:FF:FF:01**, **00:11:FC:FF:FF:02**, **00:11:FC:FF:FF:03** **FF:FF:FF:FF:FF:FF**
Domain Name	Freely selectable
Ring Port 1,2	Ports, which form the ring
Domain VLAN ID	Select the VLAN in which MRP operates. (**1** ... **4094**)
Recovery Time	Set the recovery time of the ring. (**200 ms** or **500 ms**)

Note

- Each port can only be member in one ring.
- 3 rings can be set up on a redundancy master.
- All rings must have different VLAN IDs and Domain.
- In addition, the VLANs must be created prior to setting up the MRP-rings in the VLAN menu.
- It is recommended to change the port settings to 100MBit/s full duplex for the Ring Ports.

Multi-master operation

In the case of two masters, the one with the lower priority is the master and the other client. If both are equal priorities, the MAC address is used for comparison.

The ring master with the higher MAC address remains Ringmaster.

Priority: **(0 ... 61440)**

10.2.2 MRP Status

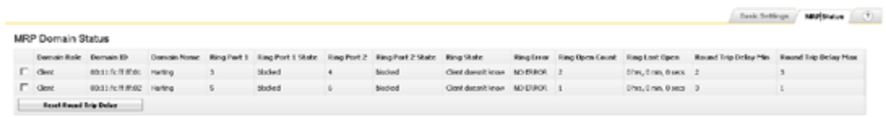


Figure 10-7 MRP Domain Status window

The following status information is shown:

Function	Description
Domain Rule	Client / Manager
Domain ID	Shows the selected Domain ID
Domain Name	Shows the selected Domain Name
Ring Port 1	Number of the ring port
Ring Port 1 state	Forwarding, blocked
Ring Port 2	Number of the ring port
Ring Port 2 state	Forwarding, blocked
Ring Status	*STATE OPEN* / *CLOSED* (Ringmaster)
Ring Error	*NO ERROR*

Note

The client can make no statement about the status ring.

11. VLAN

VLANs (Virtual LANs, Virtual Local Area Networks) can be viewed as a group of devices on different physical LAN segments which can communicate with each other as if they were all on the same physical LAN segment, that is, a network of computers that behave as if they were connected to the same wire-even though they may actually be physically located on different segments of a LAN.

VLAN provides the following benefits for switched LANs:

- Improved administration efficiency
- Optimized Broadcast/Multicast Activity
- Enhanced network security

This switch supports port-based VLANs (Virtual Local Area Networks) in compliance with IEEE 802.1Q. Initially, all ports on the switch are assigned to the configured default VLAN 1. Additional VLANs can be created on the switch and ports can be assigned to the new VLANs. This allows traffic from devices connected to these ports to bridge within their VLAN domains.

The VLAN window is divided into three tabbed sub-sections: *Basic Settings*, *Port Settings* and *Static VLAN*. Each of these sections is described below.

11.1 Basic Settings

Figure 11-1 VLAN Basic Settings tab

This tabbed section displays VLAN global configuration settings.

Function	Description
Learning Mode	Select the VLAN learning mode. You can enable either *IVL* (independent) or *SVL* (shared). This determines the access method to the VLAN filtering database. In *IVL*, the information learnt by one VLAN is never used by other VLANs in making forwarding decisions. As a result of this, there are separate filtering databases maintained for each VLAN. The advantage in using IVL is that security restrictions can be applied to prevent unauthorized users from learning the sources of data traffic. This mode is typically employed in situations where... **a**. end stations operate over multiple VLANs with the same MAC address or **b**. learning database size is not a constraint. In *SVL*, a global address table is used for all VLANs combined. **Range of value:** *IVL* / *SVL* **Default value:** *IVL*
Maximum VLAN ID	Displays the largest valid VLAN ID that the switch allows.
Maximum Support VLANS	Displays the maximum number of VLANs that this switch can support.
Number of VLANs in the System	Displays the active number of VLANs currently configured on the switch.

11.2 Port Settings

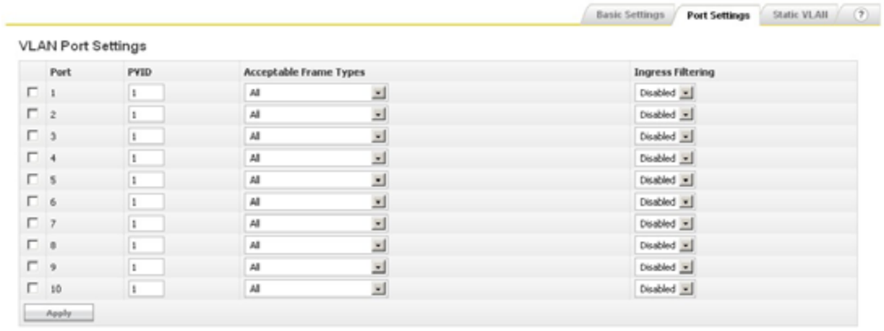


Figure 11-2 VLAN Port Settings tab

This tabbed section allows you to specify the following port settings:

Function	Description
Select/Port	This option will be checked for the port where configuration changes have been made.
PVID	Specify a port default VLAN ID (PVID) for the port for port-based VLAN classification. This is the VLAN ID which will be assigned to all untagged frames received on the port. The possible values are 1 to 4094. VLANs and assigned ports are exclusively created in the Static VLAN tab. **Range of value:** *1 ... 4094* **Default value:** *1*
Acceptable Frame Types	Select the frame types accepted (accept only tagged frames, untagged and priority tagged frames or all frames). **Range of value:** *all frames* / *only tagged frames* / *untagged and priority tagged frames* **Default value:** *all frames*
Ingress Filtering	Select if ingress (incoming) filtering is enabled or disabled at the port level. If filtering is enabled, incoming frames are discarded − in case they are tagged for VLANs which do not include this particular ingress port in their member set. If filtering is disabled, incoming frames are discarded − in case they are tagged for VLANs which are not configured on the switch. **Range of value:** *Enable* / *Disable* **Default value:** *Disable*

11.3 Static VLAN

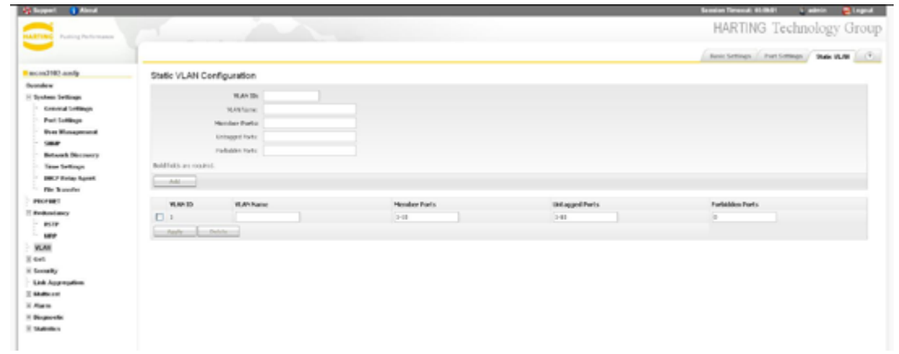


Figure 11-3 Static VLAN Configuration tab

This tabbed section displays the available VLANs and allows you to create new VLANs.

Function	Description
VLAN ID	Here you can create a new VLAN with the specified VLAN ID. Note that an existing default VLAN which includes all ports is labelled with VLAN ID 1. **Range of value:** *1 ... 4094* **Default value:** *1*
VLAN Name	Specify a user-defined name, usually used to remember the purpose of the VLAN. **Range of value:** Not more than 20 printable characters **Default value:** none
Member Ports	Specify the ports that belong to the VLAN that you are creating. **Range of value:** *All* **Default value:** *None*
Untagged Ports	Specify ports which forward packets untagged. **Range of value:** *All* **Default value:** *None*
Forbidden Ports	Specify ports which may not be included in the VLAN. **Default value:** none

After all necessary entries are made, a list will be displayed at the bottom of the window. It includes all existing VLANs along with the user-defined information. The values in this table can be changed to alter the properties of existing VLANs (the name, member ports, untagged ports or forbidden ports).

12. Quality of Service

Quality of Service (QoS) is a technology for managing network traffic in a cost effective manner to enhance network performance and reliability of the application. QoS allows the priorization of the network traffic to assure quality and performance at any time. For example, QoS technologies can be applied to prioritize traffic for latency-sensitive applications (such as automation protocols and voice or video) and to control the impact of latency-insensitive traffic

IEEE 802.1p is a standard of the IEEE, which regulates the transport of data of different priority in computer network. The standard works on the 2nd level of the OSI reference model. The transferred frames are divided into priority classes from 1 to 7. The 0 is used for frames, which are not assigned to a certain priority. The standard only specifies that the priority from 1 to 7 rises, however there are no statements about how the frames have to be treated in detail.

The priorities are coded by an additional field of the VLAN tags (TCI, see IEEE 802.3 Tagged MAC Frame). The prioritization of the frames is necessary to guarantee small latency. Applications such as Voice of over IP get a high priority, in order to keep latency and jitter small, while other applications with smaller requirements receive lower priorities. 802.1p is used in the following standards: IEEE 802.1D and IEEE 802.1Q.

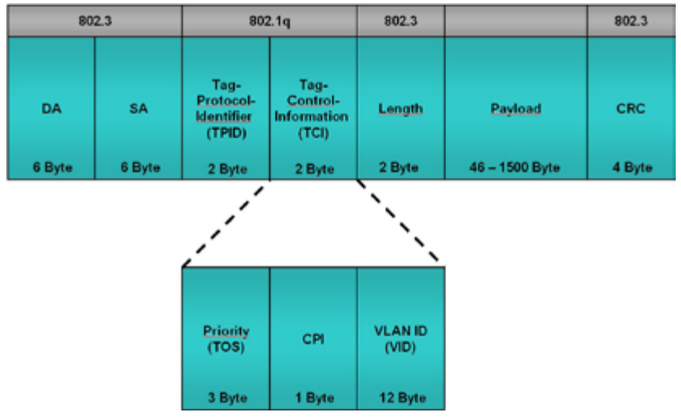


Figure 12-1 Quality of Service – Tag Control Information (TCI)

DiffServ uses the first six bits already existing in the type of the service field (ToS) of the IPv4 protocol or the Class Field in the IP header of the IPv6 protocol for signaling. To the demarcation opposite the earlier ToS or Class Field byte is designated than Differentiated services code POINT (DSCP).

12.1 Basic Settings

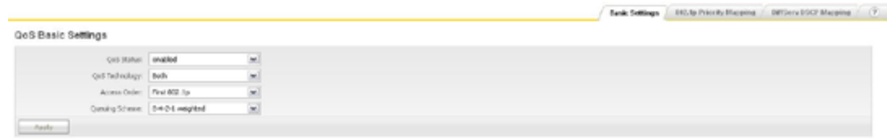


Figure 12-2 QoS Basic Settings

Function	Description
QoS Status	Enables or disables Quality of Service
QoS Technology	Set the QoS technology which should be used *802.1p*, *DiffServ* or *Both*. If both technologies are used the access order has to be set. **Range of value:** *802.1p* / *DiffServ* / *Both* **Default value:** *Both*
Access Order	Set the access order for QoS. **Range of value:** *First 802.1p* / *First DiffServ* **Default value:** *First 802.1p*
Queuing Scheme	*Strict Priority Queuing* If selected, the switch operates using a fixed priority scheme as follows: Packets in queue 0 will be forwarded as quickly as possible and this will carry on until queue 0 is empty. Only then will queue 1 be processed. If queue 0 and queue 1 are empty then queue 2 will be processed. Queue 3 will only be processed when queues 0 to 2 are empty. This scheme contains the risk that queue 3 will never be processed, as long as higher priority packets are available. *8-4-2-1 Weighted* If selected, the switch operates using a weighted priority scheme whereby the queues are tested according to the following priorities or weights: queue 0 is processed with weight 8, queue 1 has weight 4, queue 2 has weight 2, and queue 3 has weight 1. The process ensures that all queues will be continually scanned. **Range of value:** *Strict Priority Queuing* / *8-4-2-1 Weighted* **Default value:** *8-4-2-1 Weighted*

12.2 802.1p Priority Mapping

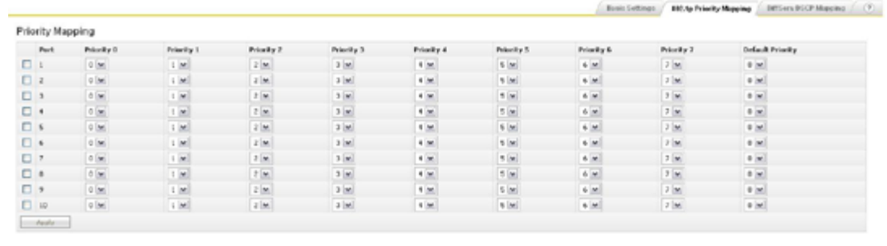


Figure 12-3 802.1p Priority Mapping tab

12.2.1 Priority Mapping

The table in this tabbed section allows you to configure the traffic class associated with each priority class for each port. Packets leaving the switch will be allocated to the queue defined in this table. The priority of each packet leaving the switch is checked and then associated with the appropriate queue. An internal traffic class between 0 and 7 may be assigned for each priority on each port.

In the columns (0-7), you can specify the priorities for incoming packets corresponding to each of the rows (ports 1-10). The default priority values are compliant with IEEE 802.1p.

For example, if a packet enters on port 1 with a level 6 priority, it will normally be processed with priority 6. However, you can specify a different processing priority within the switch by selecting a different priority (*Port 1* row, in the *Priority 6* column). The packet itself is not altered – only the processing priority within the switch.

12.2.2 Default Priority

All packets that ingress the switch without a priority tag will receive the priority selected by the drop-down menu. The priority tag will be written permanently to the packet until it is deleted by another Ethernet device.

12.3 DiffServ Priority Mapping

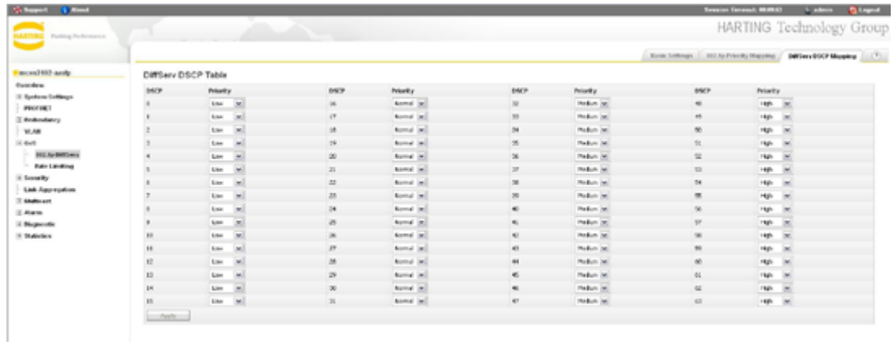


Figure 12-4 DiffServ Priority Mapping tab

This table configures the DSCP handling for Differentiated Services. Packets with a value inside the DSCP field will be put into the switching queue configured via this table.

12.4 Rate Limiting

The Rate Control feature protects the switch from packet flooding caused by malicious users. Traffic that exceeds a configured threshold traffic rate must be dropped. Rate control can be applied on flooded Unicast, Multicast and Broadcast traffic. By applying rate control on Broadcast Traffic, Broadcast Storm can be prevented. The threshold and the type of packet which should be filtered can be set separated for each port of the switch.

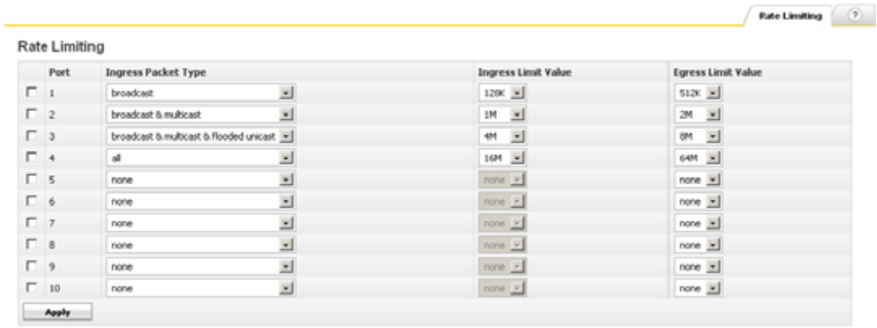


Figure 12-5 Rate Limiting

Function	Description
Ingress Packet Type	This option defines the kind of traffic which will be affected by the filtering options for this port. **Range of value:** *None* / *Broadcast* / *Broadcast & Multicast* / *Broadcast & Multicast & Flooded Unicast* / *All packets* **Default value:** *None*
Ingress Limit Value	Select the bandwidth limit for the incoming traffic on this port. **Range of value:** *128 Kbit/s* / *256 Kbit/s* / *512 Kbit/s* / *1 Mbit/s* / *2 Mbit/s* / *4 Mbit/s* / *8 Mbit/s* / *16 Mbit/s* / *32 Mbit/s* / *64 Mbit/s* / *128 Mbit/s* / *256 Mbit/s* **Default value:** *None*
Egress Limit Value	Select the bandwidth limit for the outgoing traffic on this port. **Range of value:** *128 Kbit/s* / *256 Kbit/s* / *512 Kbit/s* / *1 Mbit/s* / *2 Mbit/s* / *4 Mbit/s* / *8 Mbit/s* / *16 Mbit/s* / *32 Mbit/s* / *64 Mbit/s* / *128 Mbit/s* / *256 Mbit/s* **Default value:** *None*

Note

The adjustable values (note **range of values**) can vary according to each configured port speed.

13. Security

13.1 IP Authorized Manager

This section allows you to define an incoming IP address that is allowed access to the switch (thus functioning as an IP-based access control list). This rule also restrict which SNMP managers can access the switch MIB. The access control list of user-defined IP address is then displayed at the bottom of this section.

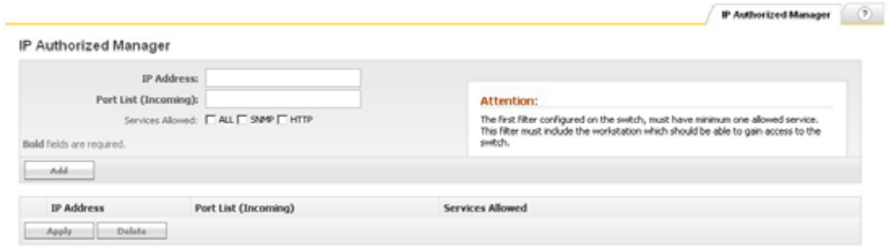


Figure 13-1 IP Authorized Manager

Function	Description
IP Address	Specify IP addresses that you wish to allow to gain access to the switch configuration. This IP address has to be an address of an existing device and no subnet or network address. All addresses which are not entered to the authorization list will be blocked.
Port List	Specify the port numbers (i.e. 3-7,9) which will be controlled by the rule. At least one port must be specified.
Services Allowed	Specify which services should be allowed or denied. If you are creating a Deny rule, no boxes should be checked.

The access control list is displayed at the bottom of the page. Incoming packets are then checked against this list and the first applicable rule is applied.

Note

Do not use a subnet or network address. Only Host IP addresses are allowed!

ATTENTION

The first filter must include the workstation which is being used to gain access to the switch. If you accidentally create a Deny rule that locks you out of the switch, it is sufficient to reboot the switch to revert back to the last set of functional filter rules.

Example: Open access for a single station

Source IP of the station which should have access to the switch: 192.168.5.101

Authorized Manager IP entered at the Authorized Manager: 192.168.5.101

13.2 Port based network access control IEEE 802.1x

The Port based Network Access Control (PNAC) is based on the IEEE 802.1X standard. It provides an authentication mechanism for devices that want to connect to a network. It prevents access to a port in cases when the authentication and authorization fails. The entity that facilitates authentication of other entities attached to it is called an Authenticator. The entity that is being authenticated by an Authenticator attached to the other end is called a Supplicant. Authentication, Authorization and Accounting for a user session with the remote Server, is done by RADIUS. The switch acts as a RADIUS client. It encapsulates the accounting information passed by the User in the required format and sends the packet to the designated RADIUS accounting server.

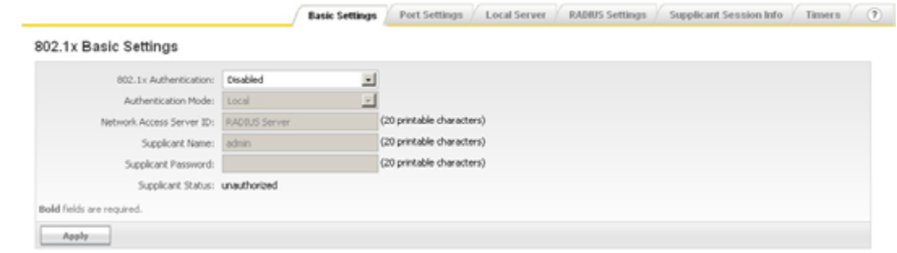


Figure 13-2 802.1x Basic Settings tab

The 802.1x Basic Settings page allows you to configure the basic settings of 802.1x.

Function	Description
802.1xAuthentication	Specifies the status of 802.1x based port security feature in the switch. Options are: *Enable* – enables 802.1x port security feature. *Disable* – disables 802.1x port security feature. **Range of value:** *Enable* / *Disable* **Default value:** *Disable*
Authentication Mode	Specifies the Authentication Server Location. **Range of value:** *Local* / *Remote* **Default value:** *Local*
Network Access Server ID	Specifies the Authenticator ID, which originates the Access-Request Packets. **Range of value:** Not more than 20 printable characters. **Default value:** *RADIUS Server*
Supplicant Name	**Range of value:** Not more than 20 printable characters. **Default value:** *admin*
Supplicant Password	**Range of value:** Not more than 20 printable characters. **Default value:** *none*

13.2.2 Port Settings

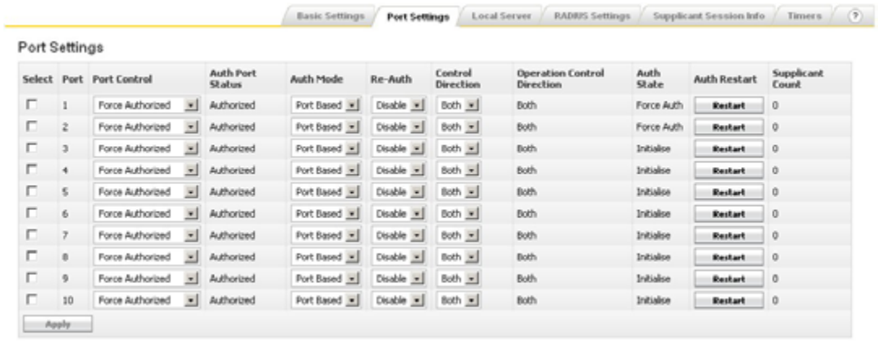


Figure 13-3 Port Settings tab

The 802.1x Port Settings page allows you to configure the security information at the individual port levels.

Function	Description
Port Control	Specifies the control values of the Authenticator Port. Options are: *ForceAuthorized* – allows all the traffic through this port. *ForceUnauthorized* – blocks all the traffic through this port. *Auto* – Imposes 802.1x authentication process in this port. **Range of value:** *ForceAuthorized* / *ForceUnauthorized* / *Auto* **Default value:** *ForceAuthorized*
Auth. Port Status	Shows the current status of the Authenticator Port. **Range of value:** *Authorized* / *Unauthorized*
Auth. Mode	Specifies the configuration for selecting the authentication mode. **Range of value:** *Port Based* / *MAC Based* **Default value:** *Port Based*

Note

In order to use MAC Based, Port Control has to be set to *Auto*.

Function	Description
Re-Auth.	Re-Auth. enables / disables re-authentication mechanism on the port. **Range of value:** *Enable* / *Disable* **Default value:** *Disable*
Control Direction	Specifies the current value of the administrative controlled directions parameter for the port. **Range of value:** *Both* / *In* **Default value:** *Both*
Operation Control direction	Specifies the current value of the operational controlled directions parameter for the port.
Auth. State	Shows the current status of the Authenticator Port. **Range of value:** *Authorized* / *Unauthorized* / *Disconnected* / *Connecting* / *Authenticating* / *Authenticated* / *Aborting* / *Held* / *ForceAuth* / *ForceUnAuth*

Function	Description
Auth. Restart	Authentication Restart specifies the initialization control for the port to restart authentication. Options are: *Start* – causes the Port to be initialized. *False* – reverts to False once initialization is complete. **Range of value:** *True* / *False*
Suplicant Count	Number of supplicants authorized on the switch

13.2.3 Local Server

Figure 13-4 Local Server tab

The Local Authentication Server Configuration page allows you to configure the Local Authentication Server information.

Function	Description
User Name	Specifies the identity of the user, seeking authentication. **Range of value:** Not more than 20 printable characters **Default value:** none
Password	Specifies the password specific to the user name. **Range of value:** Not more than 20 printable characters **Default value:** none
Port List	Represents the complete set of ports of the authenticator to which the user is allowed. **Default value:** *All*

13.2.4 RADIUS Settings

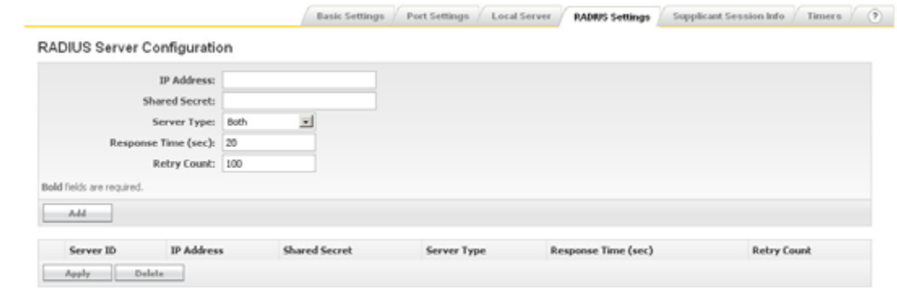


Figure 13-5 Radius Server Configuration tab

The RADIUS Server Configuration page allows you to configure the RADIUS Server information.

Function	Description
IP Address	Specifies the IP Address of the RADIUS Server.
Shared Secret	Specifies the secret string, which is to be shared between the RADIUS Server and the RADIUS Client. **Range of value:** Not more than 20 printable characters. **Default value:** none
Server Type	Specifies the RADIUS server type **Range of value:** *Authenticating* / *Accounting* / *Both* **Default value:** *Both*
Response Time	Specifies the maximum time within which the Radius Server has to respond to a request from the Radius Client. **Range of value:** *1 ... 120 sec* **Default value:** *20 sec*
Retry Count	Specifies the maximum number of times a radius request is to be re-transmitted before getting response from the Radius Server. **Range of value:** *1 ... 254* **Default value:** *100*

13.2.5 Supplicant Session Info

Figure 13-6 Supplicant Session Info tab

The Supplicant session info page displays the Supplicant Session information details.

Function	Description
Supplicant MACAddr	Specifies the Supplicant MAC Address.
Session Identifier	Specifies the Session Identifier of the supplicant.
Auth State	Specifies the state of the Authenticator State Machine.
Auth Session Status	Specifies the Authentication Session Status.
Session Port Number	Specifies the port number through which a particular Session MAC address is learnt.

13.2.6 Timers

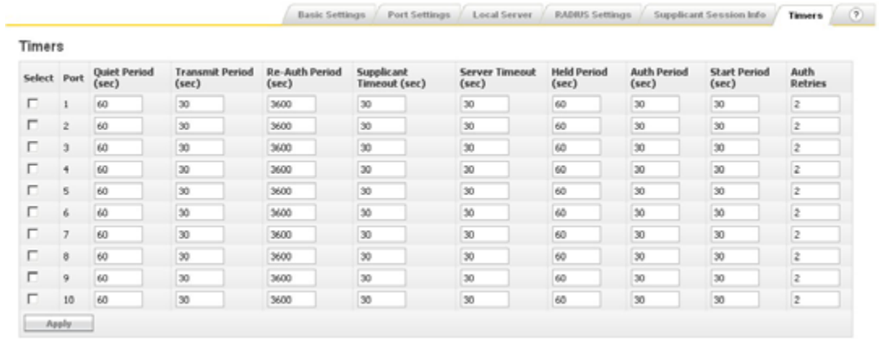


Figure 13-7 Timers tab

The 802.1x Timer Configuration page allows you to configure the *Timer* parameters at the individual port level.

Function	Description
Quiet Period	Specifies the duration for which the authenticator remains silent and will not attempt to acquire a supplicant. **Range of value:** *0 ... 65 535 sec* **Default value:** *60 sec*
Transmit Period	Specifies the time period used by the authenticator to define when the EAPOL PDU has to be transmitted. **Range of value:** *1 ... 65 535 sec* **Default value:** *30 sec*
Re-Auth. Period	Specifies the time between periodic re-authentication of the supplicant. **Range of value:** *1 ... 65 535 sec* **Default value:** *3600 sec*
Supplicant Timeout	Specifies how long the switch waits for a response before re-transmitting the request to the client if a request is relayed from the authentication-server to the client. **Range of value:** *1 ... 65 535 sec* **Default value:** *30 sec*
Server Timeout	Specifies how long the switch waits for a response before re-transmitting the request to the authentication server if a request is relayed from the client to the server. **Range of value:** *1 ... 65 535 sec* **Default value:** *30 sec*
Held Period	Specifies the amount of time the client will wait before re-attempting a failed 802.1X authentication. **Range of value:** *1 ... 65 535 sec* **Default value:** *60 sec*
Auth Period	Specifies the time interval for resending 802.1X request messages after not receiving a response. **Range of value:** *1 ... 65 535 sec* **Default value:** *30 sec*

Function	Description
Start Period	Specifies the time interval for resending Start messages. **Range of value:** *1 ... 65 535 sec* **Default value:** *30 sec*
Auth. Retries	Specifies the number of times the switch sends an EAP-request/ identity frame before restarting the authentication process. **Range of value:** *1 ... 10* **Default value:** *2*

14. Link Aggregation

The *Link Aggregation* feature allows one or more individual links (of the same speed) in the switch to be aggregated together to form a Link Aggregation Group. The switch can treat the Link Aggregation Group as if it were a single link. Link Aggregation provides: Increased bandwidth, Link redundancy and Load sharing on the individual links. Without Link Aggregation, it is difficult to have multiple links between two Ethernet stations. (R)STP disables parallel paths to prevent “loops” in the network. An end station could have multiple Ethernet links only if the links were attached to different networks. Link Aggregation resolves this limitation by allowing multiple parallel links between any two Ethernet stations.

The aggregators are automatically configured using the Link Aggregation Control Protocol (LACP). This protocol performs the basic sanity checks to see whether:

- All member links are operational
- The data rates of the member links are of the same value.
- All member links are interconnected between two identical end nodes.

Once the above checks have been carried out, LACP initiates the link aggregation. When aggregation is up, LACP periodically checks the functionality of all member links. If any member link goes down, it is removed from the aggregation. The link will be added automatically to the aggregator, as soon as the link becomes functional again.

This section allows you to define and configurate the Link Aggregation feature. Link Aggregation or trunking is a feature, which allows the combining of several physical network links into a single logical link. This trunking group will be treated as a normal port inside the switch.

14.1 Basic Settings

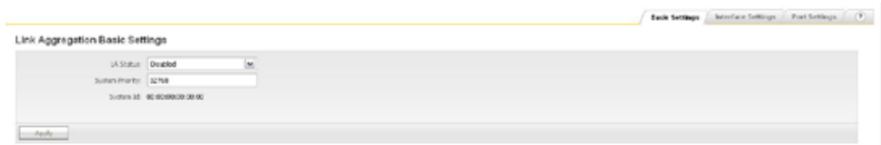


Figure 14-1 Link Aggregation Basic Settings tab

Function	Description
Link Aggregation Status Specifies	The Link Aggregation module administrative status. Options are: *Enabled* Enables Link Aggregation in the switch. *Disabled* Disables Link Aggregation in the switch. **Range of value:** *Enable* / *Disable* **Default value:** *Disable*
System Priority	Defines the system priority. **Range of value:** *0 ... 65 535* **Default value:** *32 768*
System Id	Shows the system ID (MAC Address).

14.2 Interface Settings

Figure 14-2 Link Aggregation Interface Settings tab

Function	Description
Port Channel ID	The port channel ID describes the interface declaration of the trunking group. A trunking group (Port Channel) will be treated as a normal port inside the switch. **Range of value:** *1 ... 65 535*
Admin Status	Administrative control of a Port Channel: specifies the Admin status of the port channel. **Range of value:** *Up* / *Down* **Default value:** *Down*
Oper State	Specifies the operational status of the port channel. This is a read-only field.
	All port channels are shown in the table. Each channel can be shutdown or deleted individually by the administrator.
Mode	Link Aggregation can be configured in two different ways: *Manual* and *LACP*. The *Manual* configuration will set the specific ports immediately to work as a trunk port. If the ports on the neighbour switch are not configurate as manual ports, the connections may cause loops. To minimize the appearance of failures during the configuration of manual Link Aggregation, the switches should be configurated without using redundant connections. The *dynamic* configuration with the LACP will set the specific ports to a negotiation state before acting as a trunk port. If the ports on the neighbour switch are not configurated as LACP ports, no loops or failures will occur. **Range of value:** *Manual* / *LACP* / *Disable* **Default value:** *Disable*
Ports	Specifies the interface indices that must be configured to be members of the Port Channel.
No of Ports Per Channel	Indicates the number of ports that are bundled per port channel.

14.3 Port Settings

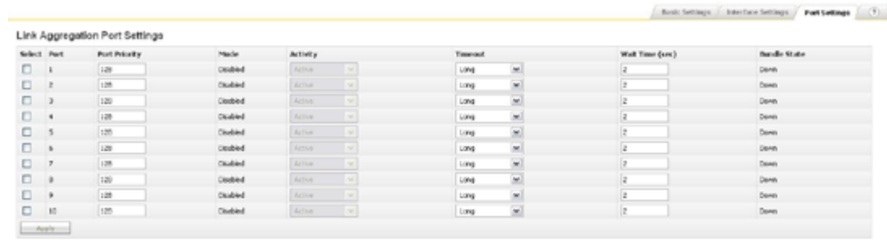


Figure 14-3 Link Aggregation Port Settings tab

Function	Description
Port	Specifies the Interface Index.
Port Priority	Specifies the Priority value of the port. If the number of links in an aggregation exceeds the maximum supported by the hardware, the links with lower priority become active links. **Range of value:** *0 ... 65535*
Mode	Link Aggregation can be configured in two different ways: *Manual* and *LACP*. The *Manual* configuration will set the specific ports immediately to work as a trunk port. If the ports on the neighbour switch are not configurate as manual ports, the connections may cause loops. To minimize the appearance of failures during the configuration of manual Link Aggregation, the switches should be configurated without using redundant connections. The dynamic configuration with the *LACP* will set the specific ports to a negotiation state before acting as a trunk port. If the ports on the neighbour switch are not configurated as LACP ports, no loops or failures will occure.
Activity	Specifies the Port LACP Activity. Options are: *Active* and *Passive*. *Active*: LACP negotiation is started un-conditionally *Passive*: LACP negotiation is started only when LACP packet is received from peer **Range of value:** *Active* / *Passive* **Default value:** *Active*
Timeout	Specifies the time within which LACP PDUs must be received on a port to avoid timing out of the Aggregated Link. Options are: *Long:* The ports will time out of the Port channel in 90 seconds. *Short:* The ports will time out of the Port channel in 3 seconds. **Range of value:** *Long* / *Short* **Default value:** *Long*

Function	Description
Wait Time(secs)	Specifies the waiting time for a port after receiving Partner information and before entering aggregation. Configuring the wait-time value as 0 ensures that links get aggregated immediately. **Range of value:** *0 ... 10 sec* **Default value:** *2 sec*
Bundle State	Indicates the current state of the port with respect to Link Aggregation. Options are: *Up In Bundle:* The port is an active member of the Port channel. *Up Individual:* The port is not a member of any port channel but its Oper-Status is *Up*. *Standby:* The port is a member of the port channel but is currently in standby state. *Down*: The Ports Oper-Status is *Down*.

15. Multicast

15.1 Multicast IGMP Snooping

The IGMP Snooping feature in helps the switch to control IPv4 multicast traffic in a switched network. A Layer 2 switch by default, floods multicast traffic within the broadcast domain. This can consume a lot of bandwidth if many multicast servers are sending streams of data. IGMP Snooping is meant to dynamically discover the presence of multicast receivers and use the learnt information to control the multicast traffic flow, restricting it only to the desired ports on which receivers are present.

The IGMP Snooping switch examines or snoops IGMP packets sent between the hosts (Multicast source) and the router. It also identifies the Multicast Group membership of the hosts. The Ha-VIS mCon Ethernet Switch learns the multicast forwarding information through the IGMP report messages from hosts and updates the Forwarding database. It also learns the router ports through the multicast control messages from the routers or Querier switch. The IGMP Snooping switch forwards multicast data traffic over a particular port only if at least one host has joined that particular multicast group. HARTING provides a dynamic multicast registration support through IGMP snooping (for IPv4 multicast traffic). IGMP snooping can be used for Layer 2/3 traffic and provides a much greater degree of granularity in selecting multicast traffic. It is possible to manually edit and add information to the forwarding database, so there is no limitation and restriction for the network topology and the application.

This section allows you to enable and configure the switch's IGMP (Internet Group Management Protocol) snooping capabilities. IGMP snooping can be used to limit high-bandwidth tasks to their intended targets without flooding the entire LAN.

Note

GMRP and IGMP Snooping cannot operate at the same time!

The following tabbed sections are available:

15.2 Basic Settings

Figure 15-1 IGMP Snooping Basic Settings tab

Function	Description
IGMP Snooping Status	Select *Enable* to enable IGMP snooping globally throughout this switch. If this setting is disabled, no interface configuration is possible. **Range of value:** *Enable* / *Disable* **Default value:** *Disable*
Operational Status	Displays the global status of IGMP snooping on the switch.
Report Forwarding	Select whether the IGMP reports to be forwarded on all ports or on router ports only. **Range of value:** *All ports* / *Router ports* / *None-Edge ports* **Default value:** *All ports*

Function	Description
Querier Forwarding	Select whether the IGMP Querier is forwarded on all ports or only on none router ports. **Range of value:** *All ports / Non Router ports* **Default value:** *All ports*
Query Transmit on TC	Select *Enabled* or *Disabled* to specify whether IGMP snooping queries are transmitted after a topology change. *Enabled* activates query transmissions. **Range of value:** *Enable* / *Disable* **Default value:** *Enable*
Sparse Mode	Select *Enabled* or *Disabled* to specify whether IGMP snooping should work in sparse or dense mode. *Enable* = Sparse Mode *Disable* = Dense Mode **Range of value:** *Enable* / *Disable* **Default value:** *Disable*

15.3 Timer

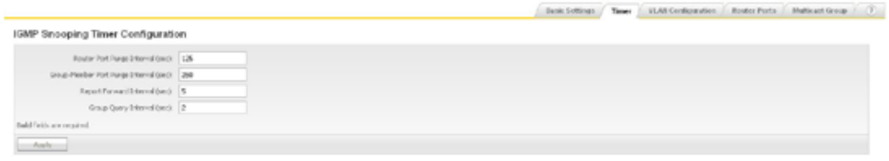


Figure 15-2 IGMP Timer tab

Function	Description
Router Port Purge Interval	Specify the interval (in seconds) at which the learnt router port will be purged. **Range of value:** *60 ... 600 sec* **Default value:** *125 sec*
Group Member Port Purge Interval	Specify the interval (in seconds) after which a port is deleted if no IGMP reports are received on that port. **Range of value:** *130 ... 1225 sec* **Default value:** *260 sec*
Report Forward Interval	Specify the interval (in seconds) before the next report messages for the same multicast group will be forwarded. **Range of value:** *1 ... 25 sec* **Default value:** *5 sec*
Group Query Interval	Specify the interval (in seconds) after which the switch sends a group-specific query on a port when an IGMPv2 leave message is received. **Range of value:** *2 ... 5 sec* **Default value:** *2 sec*

15.4 VLAN Configuration

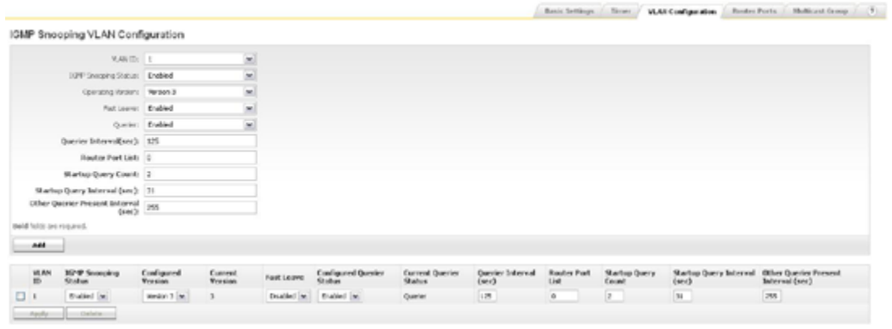


Figure 15-3 IGMP Snooping VLAN Configuration tab

This tabbed section allows you to define a specific IGMP snooping configuration for the switch. The bottom of this section displays the list of IGMP-enabled VLANs which have already been configured. The following parameters can be specified when snooping is globally enabled in the Basic Settings tab:

Function	Description
VLAN ID	Select from the list of configured VLANs to specify the VLAN to which the configuration will apply. **Range of value:** *1 ... 4094* **Default value:** *1*
IGMP Snooping Status	Select to enable or disable snooping on the specific VLAN. You can disable snooping for a specific VLAN even if snooping in enabled globally in the *Basic Settings* tab. **Range of value:** *Enable* / *Disable* **Default value:** *Enable*
Operating Version	Select the IGMP version which should be used on this switch. **Range of value:** *Version 1* / *Version 2* / *Version 3* **Default value:** *Version 3*
Fast Leave	Select whether the fast leave processing should be enabled or disabled on the specified VLAN. **Range of value:** *Enable* / *Disable* **Default value:** *Enable*
Configured Querier Status	Select whether the IGMP snooping switch should be enabled or disabled as a querier on a specific VLAN. **Range of value:** *Enable* / *Disable* **Default value:** *Enable*
Querier Interval (sec)	Specify the interval (in seconds) used to send general queries by the switch when it is configured as a querier. **Range of value:** *60 ... 600 sec* **Default value:** *125 sec*
Router Port List	Specify the router ports on the specified VLAN. All ports in VLAN 1 may be on this list (by default VLAN 1 includes all ports).

Function	Description
Startup Query Count:	The Startup Query Count is the number of queries sent out on startup, separated by the Startup Query Interval. **Range of value:** *1 ... 2* **Default value:** *2*
Startup Query Interval	Determines the interval between which the general query messages are sent by the switch during the startup of the querier election process. This value must be: ≤ *(Query Interval/4)* **Range of value:** *1 ... 60* **Default value:** *31*
Other Querier Present Interval	The Other Querier Present Interval defines how long a multicast router has to wait before it decides that there is no other multicast router, which should be the querier. **Range of value:** *1 ... 1215 sec* **Default value:** *255*

Note

The bottom of this section displays the list of IGMP-enabled VLANs which have already been configured. Changes can also be made to the list in order to modify pre-existing IGMP profiles.

15.5 Router Ports

Figure 15-4 IGMP Snooping VLAN Router Ports tab

This tabbed section displays a table showing which ports (in column 2) belong to IGMP-enabled VLANs (in column 1).

15.6 Multicast Group

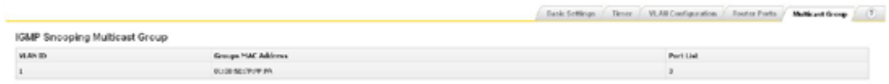


Figure 15-5 IGMP Snooping VLAN Multicast Group tab

This table displays all current multicast streams active on the switch. The VLAN ID, MAC address and port list are shown for the multicast VLAN.

16. Alarm

Certain network or switch events may require the attention of service personnel. In this section it is possible to specify certain events that should trigger an alert to be sent out.

The *Alarm* section is divided into the, *E-mail Alert* and *SNMP Alert* sub-sections.

16.1 E-Mail Alert

This section allows you to create two distinct e-mail alert profiles; these profiles are maintained in the *Alarm 1* and *Alarm 2* tabs.

16.1.1 Alarm 1 and Alarm 2

Two separate alarm profiles can be set up here. In order to activate the profiles you have to click on one or both of the *Active* boxes at the top of these tabs.

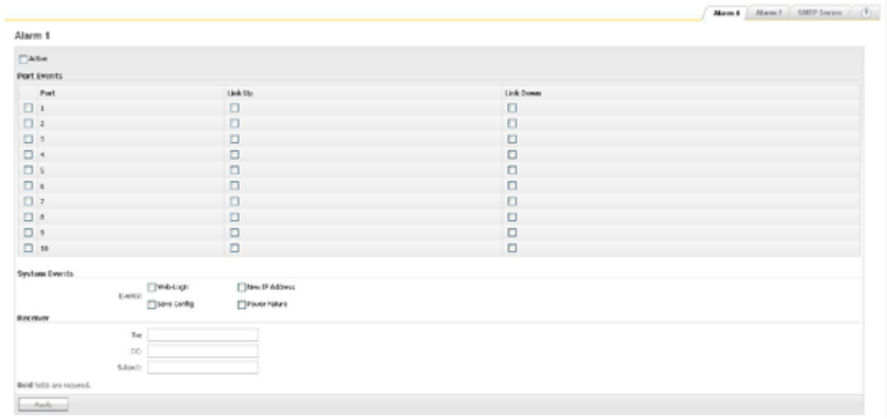


Figure 16-1 E-mail Alarm tab

Function	Description
Link Up / Link Down	Specify, on a per-port basis, if an e-mail is sent when a link is brought up or down by checking one or both of the *Link Up* and *Link Down* boxes.
System Events	Check a box next to the appropriate event: *Save Config*, *New IP address* and *Power Failure*. If a checked event takes place, it will trigger an *E-Mail Alert*.
Receiver	Specify the *To:*, *CC:* and *Subject:* fields for the alert e-mail. The SMTP server information must also be correctly specified in the next tab in order to send e-mail from the switch.

16.1.2 SMTP Server

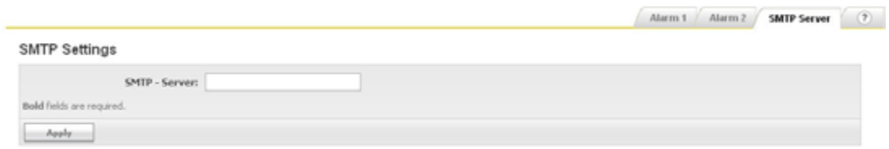


Figure 16-2 SMTP Server Settings tab

This tabbed section allows you to specify the IP address for your SMTP server here. Do not specify the server's fully-qualified domain name.

16.2 SNMP Alert

Two separate SNMP traps can be set up. You must select which profiles should be activated by clicking on one or both of the *Active* boxes at the top of this tab. Be sure to click on the *Apply* button after activating one of the trap profiles.

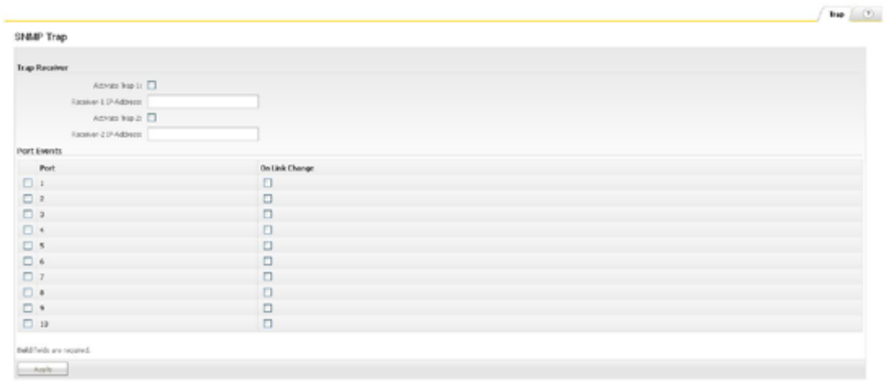


Figure 16-3 SNMP Trap section

Function	Description
On Link Change	Check this box in order to trigger an SNMP alert for the corresponding port number when the link is brought up or down. If the *Active* box is checked, then a link change on the port will trigger a trap being sent to the receiver.
Trap Receiver 1/2	Specify the IP address of an external SNMP manager that will act as the trap receiver here. This field is required.

17. Diagnostics

This section allows you to enable and view diagnostic information. Additional diagnostic information can be obtained from the power, fault and port LEDs on the switch. Refer to the **Installation Notes** for more details on the LEDs. The diagnostic sections – *Port Mirroring*, *Switch History*, *MAC Address Table*, *RMON*, *Ping* and *Light Beacon* – are described below.

17.1 RMON

Devices that are traditionally employed to study the traffic on a network as a whole are called Network Monitors/Agents. The Monitor can provide summary information including error statistics such as count of undersized packets and number of collisions and performance statistics such as the number of packets delivered per second and the packet size distribution. RMON has been designed to achieve: Proactive Monitoring Problem Detection and reporting Value Added Data. The RMON specification defines a set of statistics and functions that can be exchanged between RMONcompliant console managers and network probes. RMON provides network administrators with comprehensive network-fault diagnosis, planning, and performance-tuning information.

HARTING RMON is an implementation of Remote Network Monitoring conforming to RFC 2819.

17.1.1 Ingress Statistics

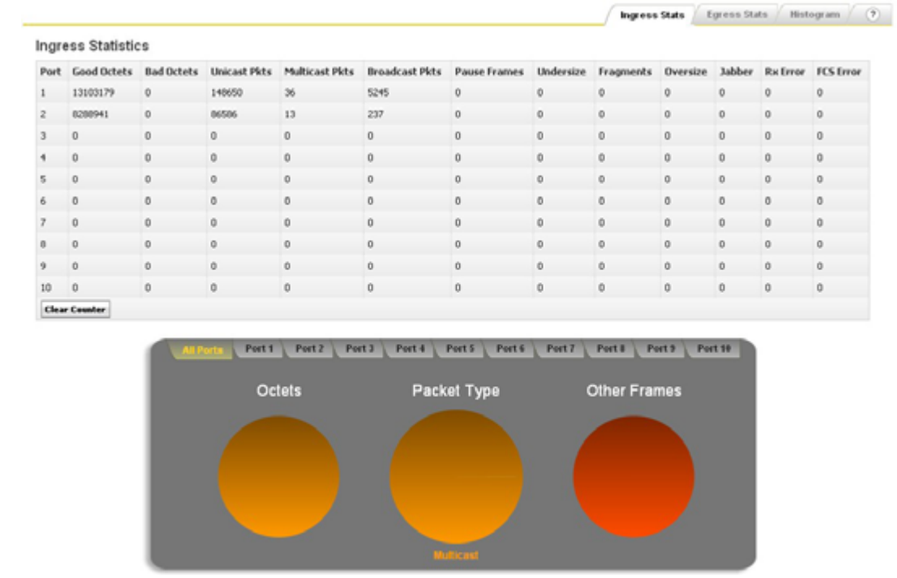


Figure 17-1 Ingress Statistics tab

Function	Description
Clear counter	This option will clear all ingress counter of the switch.
Bad Octets	Amount of bad octets received on that port
Unicast Pkts	The total number of good packets received that were directed to a unicast address.

Function	Description
Multicast Pkts	The total number of good packets received that were directed to a multicast address.
Broadcast Pkts	The total number of good packets received that were directed to the broadcast address.
Pause Frames	Amount of Pause Frames received on that port
Undersize	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of packets received that were not an integral number of octets in length or that had a bad Frame Check Sequence (FCS), and were less than 64 octets in length (excluding framing bits but including FCS octets).
Oversize	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Jabber	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and were not an integral number of octets in length or had a bad Frame Check Sequence (FCS).
Rx Error	Amount of frames received on that with an RxErr signal from the Phy
FCS Error	Amount of frames with a CRC error which was not counted by the Fragment, Jabber or RxErr counter.

17.1.2 Egress Statistics

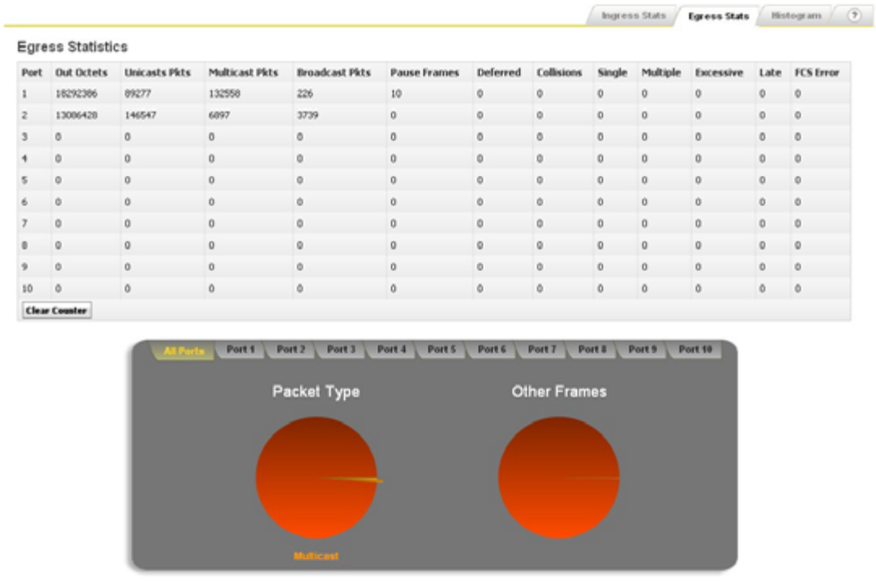


Figure 17-2 Egress Statistics tab

Function	Description
Clear counter	This option will clear all egress counter of the switch.
Out Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Unicasts Pkts	The total number of good packets sent that were directed to a unicast address.
Multicast Pkts	The total number of good packets sent that were directed to a multicast address.
Broadcast Pkts	The total number of good packets sent that were directed to the broadcast address.
Pause Frames	The total number of flow control messages that were sent.
Deferred	The total number of successfully transmitted frames with no collision but with a delay caused by a busy medium during the first attempt (only half duplex).
Collisions	The best estimate of the total number of collisions on this Ethernet segment. This counter is applicable in half-duplex only.
Single	The total number of successfully transmitted frames that experienced one collision. This counter is applicable in half-duplex only.
Multiple	The total number of successfully transmitted frames that experienced more than one collision. This counter is applicable in half-duplex only.
Excessive	The total number of frames that were dropped because the frame experienced 16 consecutive collisions. This counter is applicable in half-duplex only.
Late	The total number of late collisions (detection later than 512 bit-times into the transmission of a frame). This counter is applicable in half-duplex only.
FCS Error	The total number of frames transmitted with an invalid FCS.

17.1.3 Histogram

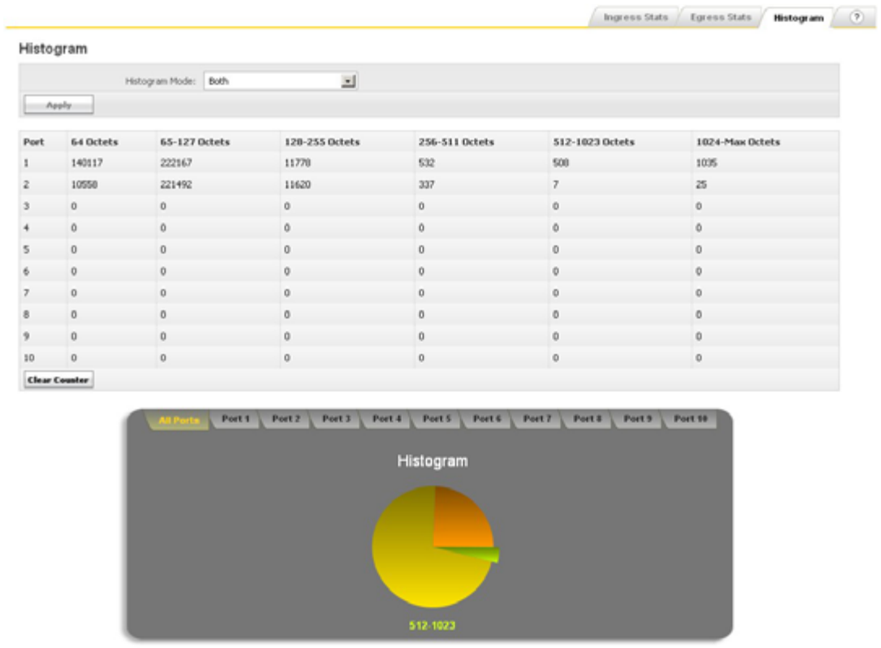


Figure 17-3 Histogram tab

Function	Description
Histogram Mode	Select the type of data which should be involved in the histogram. *Rx only*: Only inbound traffic will be shown *Tx only*: Only outbound traffic will be shown *Both*: Both, outbound and inbound traffic will be shown
64 Octets	The total number of packets (including error packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Octets	The total number of packets (including error packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255 Octets	The total number of packets (including error packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511 Octets	The total number of packets (including error packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023 Octets	The total number of packets (including error packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-Max Octets	The total number of packets (including error packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

17.2 Port Mirroring

In this tabbed section, settings are made that determine if the data traffic at a port should be mirrored to a second port for evaluation purposes. The mirrored information can then be evaluated by a network analyser.

Figure 17-4 Port Mirroring section

Function	Description
Port Mirroring Status	Select *Enabled* or *Disabled* to enable or disable port mirroring globally.

Note

Mirroring must first be activated globally; it can then be activated for the ports that you want to mirror. In this way, a maintenance configuration can be created and then activated or deactivated with this global switch.

Port	Select the port that you would like to change by clicking on the checkbox here.
Monitor Port	Select the port that you would like to use as your diagnostic (monitor) port. Only one port can be selected. This port will receive the mirrored traffic.
Mirroring Option	Select if you want to mirror the incoming traffic or the outgoing traffic or if you want to mirror both.

17.3 Switch History

This section lists a system log of all significant switch events. The one-hundred most-recent events are listed in chronological order. This list is maintained until the switch is rebooted or until the user deletes the list using the *Clear* button.

Figure 17-5 Switch History event list

Function	Description
Event No.	Switch events are numbered in decreasing order as they occur. Max. 100 events are reported.

Note

The counter starts with *1*. New events will be inserted on the first line of the list, so that the oldest event (with the lowest number) will move downwards. If more than 100 events reported, the oldest events will be deleted on the bottom line of this list.

Event No.	Switch events are numbered in decreasing order as they occur. Max. 100 events are reported.
Event	Displays a text message which describes the event which occurred.
Time / Date	Displays the time and date that the event occurred in the format hours:minutes:seconds and day.month.year.
SysUp Time	Displays the time elapsed from when the system was last powered on to when the event occurred.
Clear	Click on this button to delete the listed sequence of events. Then click on the *Switch History* tab at the top of this section to refresh the view.
Refresh	Click on this button to update the list with the most current events.

Event messages are explained in the table an p.77.

Event Message	Description
Switch History deleted	The switch history has been deleted
SYSTEM IS STARTING…	The switch is booting up
The switch has detected low supply power	A low input voltage level was detected. This message occurs as well if only one out of the two power terminals is connected.
Configuration was saved	The configuration was saved
IP address has been changed	The IP-address has changed
Web login successful	Log in to the web interface was successful
Web login expired	The web session was terminated because the web session timer has expired
Web login failure	Log in to the web interface was not successful due to wrong credentials
User admin logged in via telnet from <IP-Address>	Log in to the command line interface via telnet was successful
User admin logged out via telnet from <IP-Address>	Log out from the command line interface via telnet was successful
Attempt to login as admin via telnet from <IP-Address> failed	Log in to the command line interface via telnet was not successful due to wrong credentials
User admin logged in via ssh from <IP-Address>	Log in to the command line interface via ssh was successful
User admin logged out via ssh from <IP-Address>	Log out from the command line interface via ssh was successful
Attempt to login as admin via telnet from <IP-Address> failed	Log in to the command line interface via ssh was not successful due to wrong credentials
Firmware update was initiated	A firmware update was initiated
Firmware update failed	Updating the firmware failed
Firmware Update aborted	Updating the firmware was aborted by the user
Link status <up|down> on interface Fa 0/<port-number>	Indicates that a device was connected/ disconnected at the specific interface
Admin status <up|down> on interface Fa 0/<port-number>	Indicates that the user has enabled/disabled the specific interface
Got time from <SNTP-server-ip-address>(a.<SNTP-server-index)	Date and Time synchronised synchronized successfully with one of the configured server
Writing new <config-file> with default values	The switch was reset to the factory default settings
Set to factory default operation failed	Reset to factory defaults failed
Send email message: <message-text>	An email was successfully relayed to the SMTP-server
Send email failure: <error-message>	Sending the email failed
hTrap: <error-message>	Incorrect configuration of the SNMP-Trap alarm
PNIO: config-data has been changed	Settings, which are normally managed by the PNIO-Stack, have been changed by user
MRP: State change Sender: <Domain ID> Msg: <Ring Open|Close>	Indicate that the MRP Ring is Open or Closed
SD-Card: Config-File access failure	The configuration stored on the SD-Card could not be read

17.4 MAC Address Table

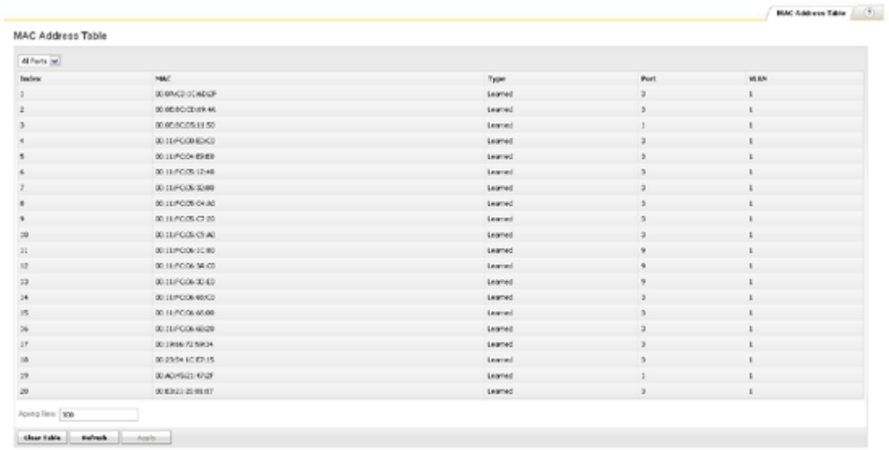


Figure 17-6 MAC Address Table

The table lists MAC (Media Access Control) addresses of devices connected to the switch. The following details and functions are available:

Function	Description
All Ports	Select which ports you want to see listed in the table. If all ports are not listed, re-select *All Ports* and click on the *Apply* button.
Index	Displays the row or sequence number of the entry.
MAC	Displays the hardware-based MAC address for the device learned through the port.
Type	Displays whether the MAC address was learned automatically by the switch or if it was entered manually. *Unlearned* is displayed when the address has been manually specified.
Port	Displays the number of the port from which the MAC address was learned.
VLAN	Indicates in which VLAN the MAC has been learned.
Ageing Time	Specify the ageing period (in seconds) after which the MAC address entry will be deleted from the table if it is no longer needed.
Clear Table	Click on this button to delete the current address/port assignments table. A new address/port table is created once again after you click to select *All Ports* at the top of this section. This feature allows you to quickly verify which devices have been replaced or added.
Refresh	Click on this button to update the information.

17.5 Light Beacon

The Light Beacon functionality is a simple method to locate and detect a specific switch inside the switchgear cabinet. For maintaining and monitoring the switch hardware, technicians often need a simple procedure to identify a switch inside the mesh. The Ha-VIS Management Software offers a feature for an easy identification via the internal Fault-LED and the Relay.

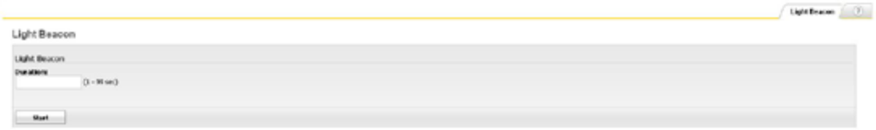


Figure 17-7 Light Beacon functionality

Function	Description
Duration	Sets the time interval for the Light Beacon functionality. **Range of value:** *1 ... 99 sec* **Default value:** none

17.6 Ping

This functionality will send ICMP packets (pings) to a specific IP-Address within the network. The result of the ping request will be shown inside the table.

Figure 17-8 Ping functionality

Function	Description
Destination	The IP-Address of the destination **Range of value:** IP-Address inside the switch subnet **Default value:** none

18. Statistics

18.1 Interface statistics

Interface (port) statistics and Ethernet statistics are displayed in the two separate tabbed sections. Counters for the statistics are refreshed each time the tab title is clicked. Counters are reset when the switch is turned off.

18.1.1 Interface Statistics

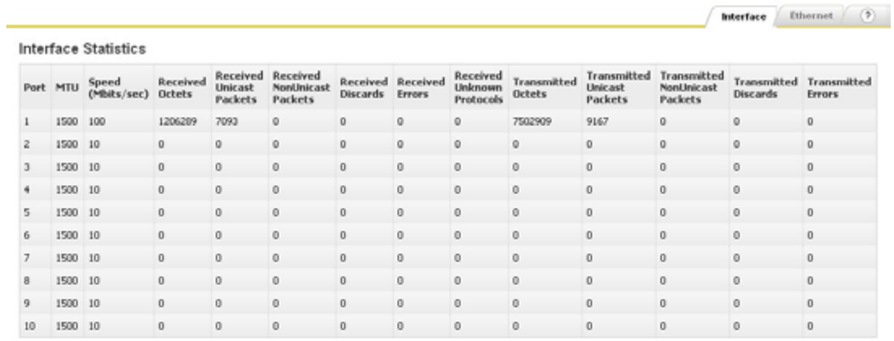


Figure 18-1 Interface Statistics tab

The *Interface Statistics* tab displays per-port device information on utilization and errors. The following columns are displayed:

Function	Description
Port	Displays the port number on the switch.
MTU	Displays the size in bytes of the MTU (Maximum Transmission Unit) for the Ethernet port.
Speed	Displays the speed of the port in bits per second. This is dependent on the media jack type.
Received Octets	Displays the number of bytes (octets) received on the port since last powered up.
Received Unicast Packets	Displays the total number of packets received with a specific destination (unicast).
Received NonUnicast Packets	Displays the total number of non-unicast packets received with no specific destination (of type *broadcast* or *multicast*).
Received Discards	Displays the number of packets received and discarded. This can occur when resources are insufficient to handle incoming traffic.
Received Errors	Displays the number of incoming packets discarded due to format errors (such as undersized, oversized, or improper-FCS packets).
Received Unknown Protocols	Displays the number of IP data packets received and discarded because of an unsupported or unknown protocol.
Transmitted Octets	Displays the total number of transmitted bytes (including bad packets) transmitted on that port.

Function	Description
Transmitted Unicast Packets	Displays the total number of packets transmitted with a specific destination (unicast).
Transmitted NonUnicast Packets	Displays the total number of non-unicast packets transmitted (of type *broadcast* or *multicast*).
Transmitted Discards	Displays the number of packets dropped due to network congestion or path error.
Transmitted Errors	Displays the number of packets discarded due to format errors.

18.1.2 Ethernet Statistics

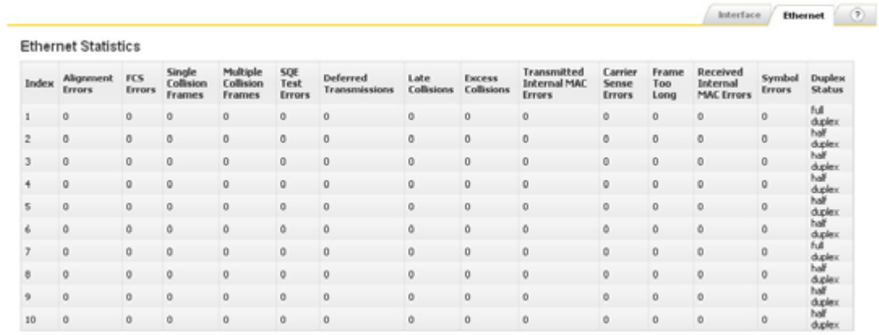


Figure 18-2 Ethernet Statistics tab

The following packet and frame errors are displayed for each port:

Function	Description
Port	Display the Port number on the switch
Alignment Errors	Displays the number of alignment errors received.
FCS Errors	Displays the number of errors involving incoming Frame Check Sequence octets.
Single Collision Frames	Displays the count of successfully-transmitted frames on the interface for which transmission is delayed by one collision.
Multiple Collision Frames	Displays the count of successfully-transmitted frames on the interface for which transmission is delayed by more than one collision.
SQE Test Errors	Displays the number of times that the SQE test error was generated for this port.
Deferred Transmissions	Displays the number of frames where the initial transmission was delayed because the medium was busy.
Late Collisions	Displays the number of times that a collision was detected at a point 512 bit-times after the packet's transmission.
Excess Collisions	Displays the number of frames on the interface for frames that failed due to too many collisions.
Transmitted Internal MAC Errors	Displays the number of frame errors where transmission failed because of an internal MAC sub-layer error.
Carrier Sense Errors	Displays the number of times the carrier sense condition was lost when attempting a frame transmission on the port.

Function	Description
Frame Too Long	Displays the number of oversized frames received on this port (frames which are larger than the maximum permissible frame size).
Received Internal MAC Errors	Displays the number of frame errors where reception failed because of an internal MAC sub-layer error.
Symbol Errors	Displays the number of received symbol errors that the switch could not decode.
Duplex Status	Displays whether half or full duplex is being used for the port.

18.2 RSTP Statistics

The two tabs in this section display information and statistics for the Rapid Spanning Tree Protocol.

18.2.1 RSTP Information

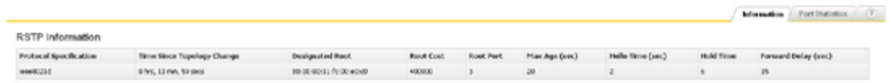
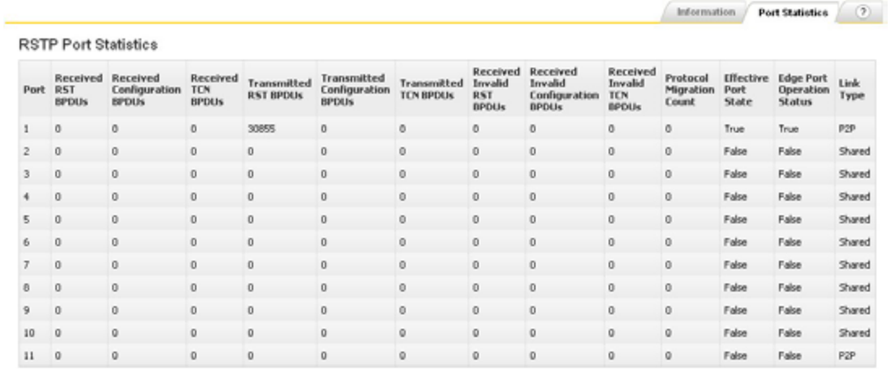


Figure 18-3 RSTP Information tab

18.2.2 RSTP Port Statistics

This tabbed section allows you to view a wide range of RSTP-related port statistics.



Port	Received RST BPDUs	Received Configuration BPDUs	Received TCN BPDUs	Transmitted RST BPDUs	Transmitted Configuration BPDUs	Transmitted TCN BPDUs	Received Invalid RST BPDUs	Received Invalid Configuration BPDUs	Received Invalid TCN BPDUs	Protocol Migration Count	Effective Port State	Edge Port Operation Status	Link Type
1	0	0	0	30855	0	0	0	0	0	0	True	True	P2P
2	0	0	0	0	0	0	0	0	0	0	False	False	Shared
3	0	0	0	0	0	0	0	0	0	0	False	False	Shared
4	0	0	0	0	0	0	0	0	0	0	False	False	Shared
5	0	0	0	0	0	0	0	0	0	0	False	False	Shared
6	0	0	0	0	0	0	0	0	0	0	False	False	Shared
7	0	0	0	0	0	0	0	0	0	0	False	False	Shared
8	0	0	0	0	0	0	0	0	0	0	False	False	Shared
9	0	0	0	0	0	0	0	0	0	0	False	False	Shared
10	0	0	0	0	0	0	0	0	0	0	False	False	Shared
11	0	0	0	0	0	0	0	0	0	0	False	False	P2P

Figure 18-4 RSTP Port Statistics tab

18.3 IGMP Snooping Statistics

18.3.1 IGS Statistics

This tab displays general IGMP statistics. Refer to RFC 2236 for detailed information concerning the statistics in these columns.

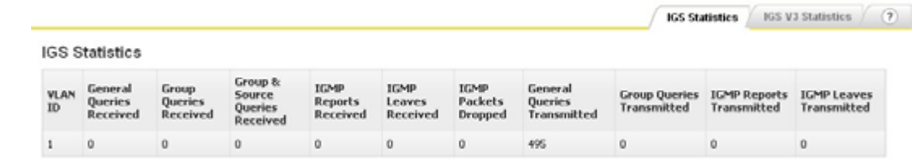


Figure 18-5 IGS Statistics tab

18.3.2 IGS V3 Statistics

This tab displays statistics that are specific to version 3 of IGMP. Refer to RFC 3376 for detailed protocol and group record type information.

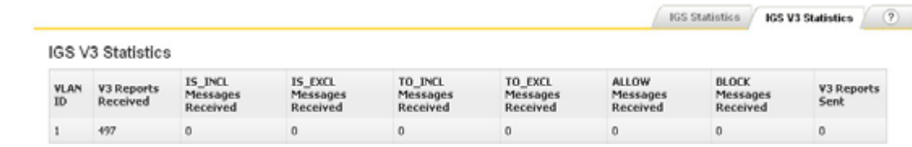


Figure 18-6 IGS V3 Statistics tab

19. SD Memory Card (optional)

The Ha-VIS mCon 3000 Next Generation switches offer the possibility to insert a SD memory card to store configurations (e.g. for maintenance purpose) and for licensing the MRP via separately available SD card.

Following SD memory cards are available:

- Configuration memory part no. 20 89 900 1000
- MRP Slave part no. 20 89 900 1001
- MRP Master part no. 20 89 900 1002

The slot to insert and eject the card is on the backside of the switch:

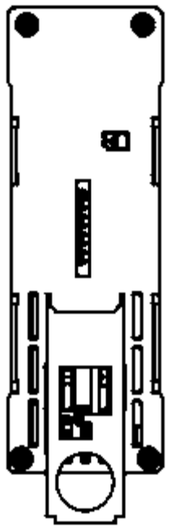


Figure 19-1 Slot for SD card on the backside of the switch

Insert an empty memory card into the slot and start the switch. The active configuration will be stored on the memory card when the ***SAVE CONFIGURATION*** Button is pushed (see chapter **6.2**).

If the inserted memory card already contains a valid configuration, the switch will load this configuration directly from the SD card.

If no card is inserted, the switch starts with the flash-memory configuration.

The card configuration will only be used during start-up process or by using the button for saving the configuration (***SAVE CONFIGURATION***, see chapter **6.2**).

Note

- In Ha-VIS mCon switches, only HARTING SD cards can be used.
- Plug in or remove the SD card only when the switch is turned off.
- At a time, only one configuration can be stored on the memory card. This configuration has a special file name.
- If a valid SD memory card is inserted and the ***SAVE CONFIGURATION*** button is pressed, the configuration will be stored inside the flash memory of the Ethernet switch as well as on the SD card
- When an SD card is plugged in, the switch stores the configuration always on the SD card and the internal flash.
- To save a configuration on the SD card it has to be unlocked.

MRP memory cards allow you to activate the MRP functionality (media redundancy protocol) when using switches from the mCon 3000 series (with firmware ver. 3.0.0.1 and later). For example, in order to operate the device as an MRP slave, you need only to have the corresponding MRP slave card inserted during operations.

20. Configuration with Automation Software Tool

The Ha-VIS mCon 3000 Next Generation Ethernet Switch supports the **PROFINET I/O** stack and can be projected via automation software tool. Following instructions refer to **Step7** as example for an automation software tool.

Settings via automation software tool and Web access:

Several settings like IP address can be made via Web access or via automation software tool. All new setting made via automation software tool overwrite old settings.

For more information about PROFINET please look at the homepage of the PROFIBUS & PROFINET International at **http://www.profibus.com/**

For more information about **Step7** please look at the homepage of the Siemens AG at **http://www.siemens.com/**

20.1 Installing the Switch as a PROFINET Device

As delivered, the switch is not a PROFINET IO device. In order to use it as a PROFINET IO device, you must activate the PROFINET functionality and download the corresponding GSD file. You can find more detailed information about how to activate PROFINET and how to download the GSD file in the PROFINET IO Stack chapter.

1. Extract the GSD file to a directory of your choice.
2. Open the hardware configuration of your development environment and navigate to Options → Install GSD File.

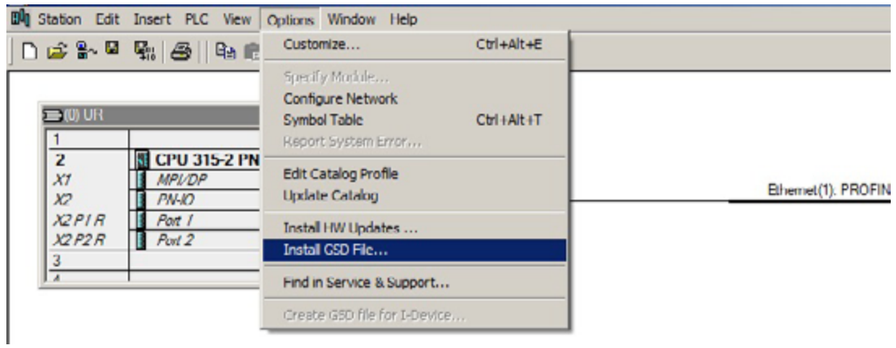


Figure 20-1 Installing the GSD file

3. Enter the path to the GSD file and select the GSD file you want to install.

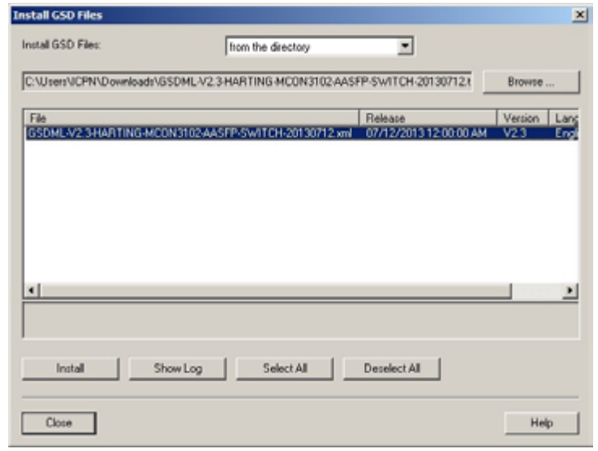


Figure 20-2 Select GSD file

4. After successful installation, the switches are available in the component library under PROFINET IO → Additional Field Devices → Switching Devices → HARTING Ha-VIS Switch.

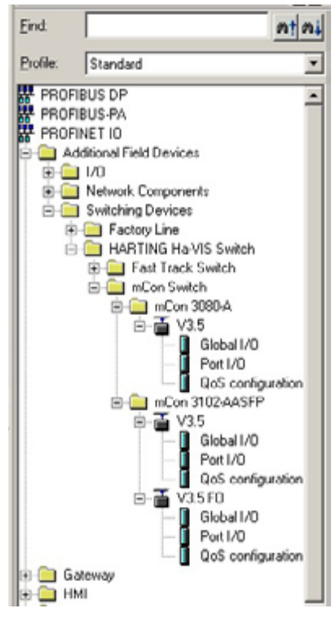


Figure 20-3 Component library

Note

There are two Ha-VIS mCon 3102-AASFP listed in the component library. Use V3.5 when you want to use both RJ45 Combo Ports. Use V3.5 FO when you want to use both SFP Combo Ports.

5. Add the desired switch by Drag and Drop into the Ethernet system.

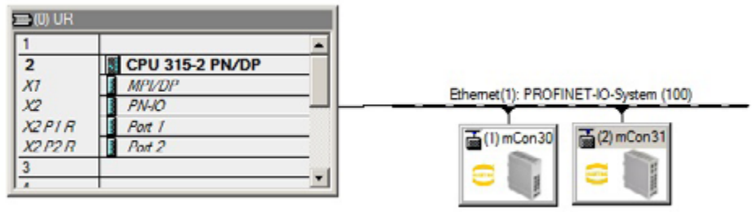


Figure 20-4 Adding a switch

6. Click on the icon to specify the device name and IP address.

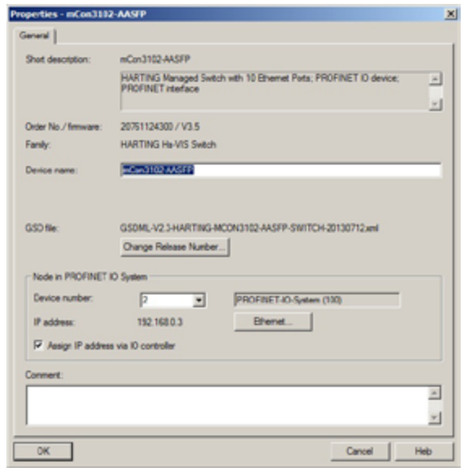


Figure 20-5 System characteristics

7. Save and compile your project and transfer it to your controller.
8. Then the switch must have its device name assigned to it. To do this, navigate in the menu PLC → Ethernet → Assign Devie Name.

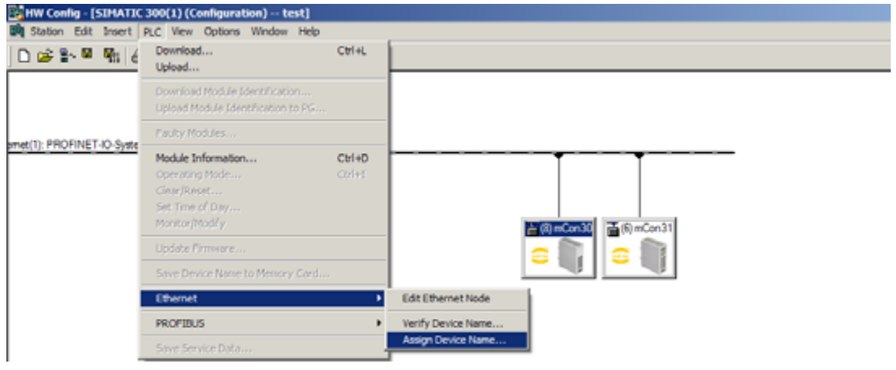


Figure 20-6 Assign Device Name

9. Select the relevant device and assign the name.

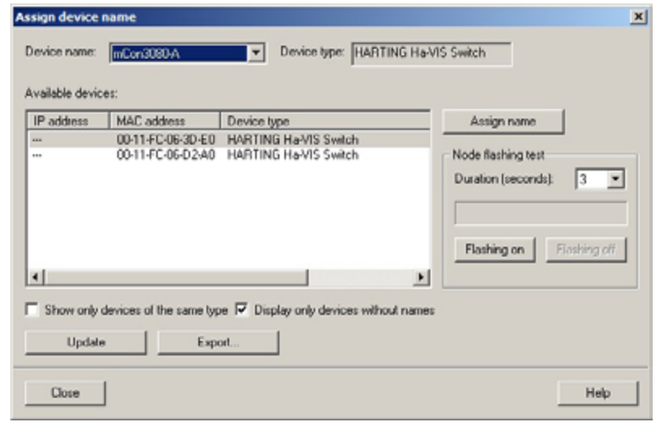


Figure 20-7 Select the switch and assign the names

20.2 Hardware Configuration

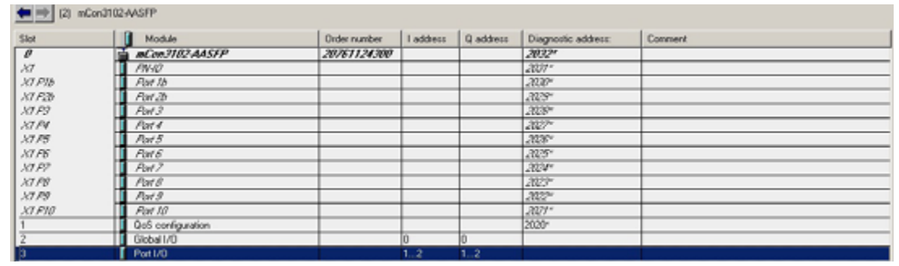


Figure 20-8 Slots and modules of the Ha-VIS mCon 3000 Next Generation switches

20.2.1 Slot 0: mCon 3080-A / mCon 3102-AASFP

Double-clicking on the module Slot 0: mCon 3080-A/mCon 3102-AASFP gets you to the properties menu.

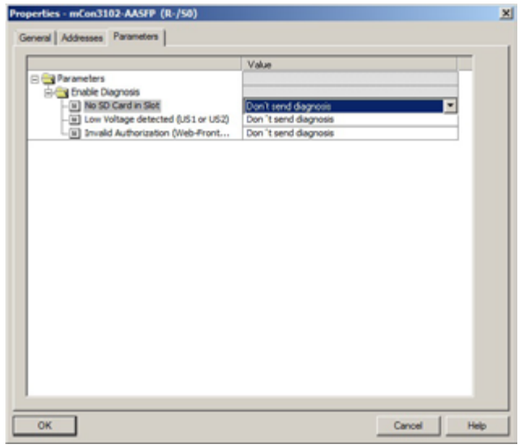


Figure 20-9 Alarms on Slot 0

Here you will find information about the device like:

- Description
- Order number
- Software version
- Device name
- Diagnostic address

In the “Parameters” tab, you can configure several diagnostic alarms, such as:

- **No SD Card in Slot**

  An alarm is triggered when the SD card is missing.

- **Low Voltage detected (US1 or US2)**

  An alarm is triggered if low voltage is detected (less than 9.6 volts) on the power supply terminals 1 or 2. This is independent of which of the two power supplies is undervoltage.

- **Invalid Authorization (Web-frontend/CLI)**

  An alarm is triggered if a user attempts to register into the web interface or CLI with false credentials.

20.2.2 Slot X1

Double click at PN-IO and the ***Properties*** will be opened.

In the tab ***General*** you can edit the name of the slot PN-I/O.

In the tab ***Addresses*** you can edit the address of that interfaces used for diagnostics.

In window ***I/O Cycle*** you can change the update time. The number of accepted update cycles with missing I/O data is set to 3.

20.2.3 Slot X1 P1 to X10 P10: Port 1-10

Here you can make adjustments for a specific port. Double-clicking the respective port opens the context menu. In the Topology tab you can set-up the connection between the devices according to your system topology.

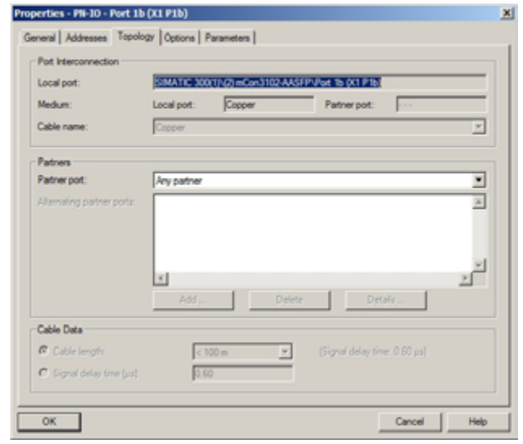


Figure 20-10 Topology settings

In the Options tab you can define the speed and the transmission medium.

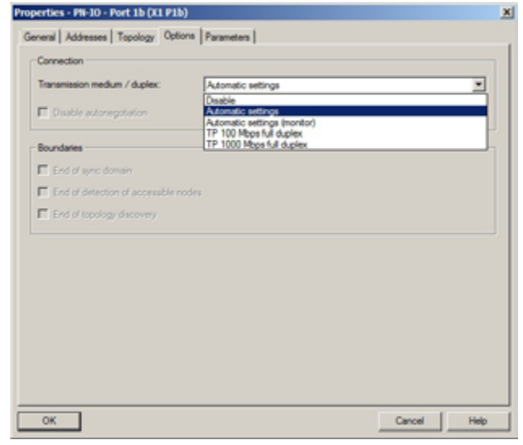


Figure 20-11 Transmission medium / duplex settings

Function	Values
Tranmission medium / duplex	Disable
	Automatic Settings
	Automatic Settings (monitor)
	TP/FO 100 Mbps full duplex (Depending on the device used)
	TP/FO 1000 Mbps full duplex (Depending on the device used)

In the Parameters tab, you can configure if you want to monitor the port and if an alarm message should be generated if there is a change to the link status, for example.

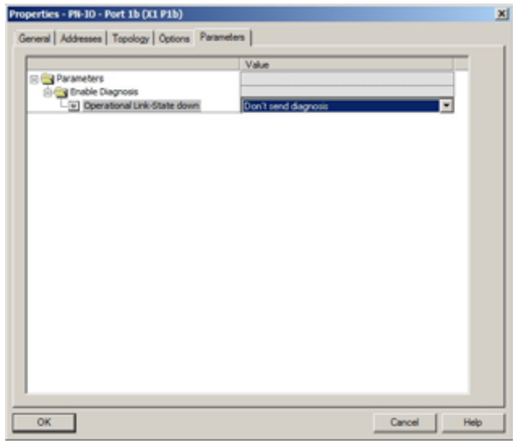


Figure 20-12 Port-related alarms

20.2.4 Slot 1: QoS Configuration

In this module you can set which QoS technology and which queuing scheme you want to use. You can find more information about QoS in chapter 11.

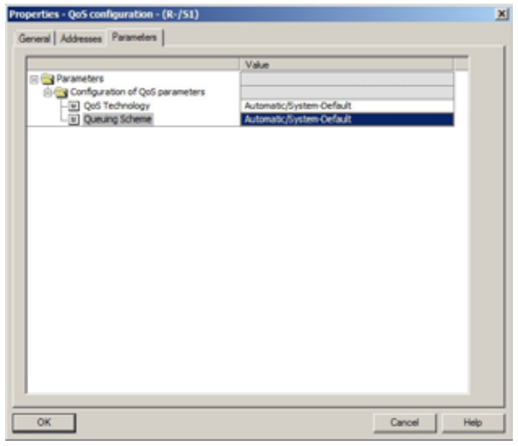


Figure 20-13 QoS settings

Function	Values
QoS Technology	Automatic/System-Default
	802.1p
	DiffServ
	802.1p and DiffServ

Function	Values
Queuing Scheme	Automatic/System-Defaults
	8-4-2-1 weighted
	Strict Priority Queuing

20.2.5 Slot 2: Global IO Data

This function gives you 1 byte for global device IO data.

Bit	Value	Meaning	Value	Meaning
0	0	-	1	No SD card inserted
1	0	-	1	Low Voltage detected (US1 or US2)
2	0	-	1	The Configuration has been changed
3	0	-	1	Log in to the web interface or CLI was not successful due to wrong credentials
4	0	-	1	-
5	0	-	1	-
6	0	-	1	-
7	0	-	1	-

20.2.6 Slot 3: Port IO

This function gives you 2 bytes for port-specific IO data for link monitoring.

		Byte 1		
Bit	**Value**	**Meaning**	**Value**	**Meaning**
0	0	Port 1 is DOWN	1	Port 1 is UP
1	0	Port 2 is DOWN	1	Port 2 is UP
2	0	Port 3 is DOWN	1	Port 3 is UP
3	0	Port 4 is DOWN	1	Port 4 is UP
4	0	Port 5 is DOWN	1	Port 5 is UP
5	0	Port 6 is DOWN	1	Port 6 is UP
6	0	Port 7 is DOWN	1	Port 7 is UP
7	0	Port 8 is DOWN	1	Port 8 is UP

		Byte 2		
Bit	**Value**	**Meaning**	**Value**	**Meaning**
0	0	Port 9 is DOWN	1	Port 9 is UP
1	0	Port 10 is DOWN	1	Port 10 is UP
2	0	-	1	-
3	0	-	1	-
4	0	-	1	-
5	0	-	1	-
6	0	-	1	-
7	0	-	1	-

Appendix

Glossary of Terms and Abbreviations

Ageing — The dating process which the Ethernet switch uses to keep track of how old certain data is. Entries in the MAC address table, for example, are deleted after they pass a certain age.

Auto-negotiation — An Ethernet mechanism which allows 10/100 Mbit/s or 10/100/1000 Mbit/s Ethernet ports to automatically establish the optimal duplex mode, flow control and speed.

Boot — The process of starting up a device and loading the operating system.

Browser — An application program running on a client PC which allows the user to view and interact with web pages on the switch or anywhere on the Internet.

Collision — The event when two packets in an Ethernet network collide. A minimal number of collisions are typical on Ethernet. A sudden prolonged increase in the number of collisions, however, may indicate that a device is experiencing a problem.

Cost — A factor used when calculating path transmission speeds. The cost of a port or path is assigned based on its desirability, with desirable (faster) paths being assigned lower costs.

DHCP (Dynamic Host Configuration Protocol) — A method for dynamically assigning IP addresses on a network. Dynamic addressing simplifies the administration of a network because the DHCP software (and not the network administrator himself) is responsible for tracking the IP address allocation. Typically, a DHCP server can be used on a LAN to “lease” an IP address to a new device for a limited amount of time. The Ha-VIS mCon Ethernet Switch is configured to accept this address when IP Address Mode is set to *Dynamic*.

Ethernet — An IEEE standard networking protocol. The protocol describes a frame-based technology for sending out and receiving from a transmission media.

Export — The process of transferring (uploading) a saved configuration or firmware file from the Ethernet switch to a TFTP server.

Fast Ethernet — An Ethernet network capable of operating at 100 Mbit/s.

Firmware — The programming code used by the switch for its basic operating functions. The Ethernet switch firmware operating system can be upgraded by overwriting it with a new firmware version.

Flow Control — A mechanism that allows high speed devices to communicate with lower speed devices. The rate of data transmission is limited when the fast sender slows down to prevent a slow receiver from being overrun with data.

Full Duplex — The ability of a network connection to handle communication in both directions simultaneously.

Gigabit Ethernet — An Ethernet network capable of operating at 1000 Mbit/s (1 Gbit/s).

Half Duplex — A network connection that is not capable of communications in both directions simultaneously. Communication in both directions is possible, but each device must wait for the other to stop transmitting before replying.

HTTP (HyperText Transport Protocol) — A communication protocol used between a web browser and web server. HTTP is used throughout the world wide web and is also used between the client web browser and the web server on the Ethernet switch.

IEEE (Institute for Electrical and Electronics Engineers) — An American organization created in 1963 that has been responsible for setting standards for communications.

IGMP (Internet Group Management Protocol) — A protocol used to manage the membership within IP multicast groups. It enables hosts to notify a local router or switch and inform them that they would like to receive transmissions assigned to a specific multicast group.

IGMP Snooping — A method where a switch listens (“snoops”) in on IGMP messages so that it can optimize the traffic flow. IGMP snooping is able to limit bandwidth-intensive traffic (such as streaming video) to only the specific requestors. Flooding of the entire network is then avoided.

Import — The process of transferring (downloading) a configuration or firmware file from a TFTP server to the Ethernet switch.

IP (Internet Protocol) — The broad-based protocol used in the Internet layer of the Internet protocol suite. The IP protocol defines addressing and data packet formats.

IP Address — A numeric address used to identify a computer or device on a network. The Ethernet switch has a default IP address of *192.168.0.126* set at the factory. A new, unique IP address should be assigned to fit the user LAN.

LAN (Local Area Network) — The group of computers and devices that populate your local network. The address range of a LAN can be defined by the subnet mask.

Link Aggregation — A trunking strategy which optimizes available resources by linking a group of ports together to form a single trunk.

MAC (Media Access Control) Address — The unique, physical address assigned to a device by the manufacturer. The switch maintains a MAC address table of connected devices. These addresses are used for sending layer-two Ethernet frames to a specific host.

Managed Switch — An intelligent device which filters and forwards packets between network segments. A managed switch features one or more ways for the user to directly access and configure switch operations (such as a web or command-line interface).

MIB (Management Information Base) — A database used by SNMP to describe and manage devices within a network.

Mirroring — A process where data flow from or to a particular port is duplicated and sent to another port for monitoring purposes.

Multicast	A method of network addressing used to deliver information to a group of targets simultaneously. Multicast addressing attempts to implement the most efficient strategy possible for delivery and creates copies of data streams only when links to multiple destinations split apart.
Packet	A discrete unit of data sent out over a network.
Port	A connection jack on a switch or device which is used for plugging in connections to other devices.
Port Mirroring	A network monitoring method where a copy of all incoming or outgoing port traffic is forwarded from one switch port to another. The duplicated traffic flow can then be analyzed at the forwarded port. The network administrator may use a protocol analyzer which captures and evaluates the data flow without influencing the client on the original port.
QoS (Quality of Service)	A control mechanism or strategy for achieving a higher quality of service. The strategy used on the Ethernet switch assigns different priority to packets from different ports. Thus, certain critical ports on the switch can be given priority over others. This can help assure better transmissions for those ports during network congestion.
Redundancy	A strategy used by the switch to provide back-up paths in the event that an active link fails. The back-up link guarantees that data transmission can continue even when the primary link goes down. RSTP is used to create a redundant network topology.
Relay	An electrical circuit that can be open or closed. The mCon Ethernet Switch uses a relay port to send out electrical signals based on the configuration in the Alarm -> Relay Alert section.
RFC (Request For Comment)	A formalized publication of the Internet Engineering Task Force describing a certain protocol or method used in Internet-based communications. RFCs can be downloaded from http://tools.ietf.org/html/.
RSTP (Rapid Spanning Tree Protocol)	A layer-two protocol that creates a spanning tree topology within a network of inter-connected bridges (such as the Ethernet switch). RSTP disables links that are not part of this spanning tree, thus creating a single loop-free path between any two network nodes.
SMTP (Simple Mail Transfer Protocol)	The standard Internet e-mail transmission protocol. A relay SMTP server should be specified on an e-mail client (such as the Ethernet switch) to enable it to send outgoing e-mails.
SNMP-Community	A SNMP group, minimally consisting of a manager and an agent. Access to the group is limited by a community string.
SNMP (Simple Network Management Protocol)	A network management system used to monitor attached devices (such as the Ethernet switch). Managed devices collect state information about themselves and make this information available to centralized network-management systems. The Ethernet switch maintains status information in its MIB which can be accessed by a separate SNMP management work station.

SNMP V1	An earlier version of SNMP where security is based only on private community strings.
SNMP V3	The current version of SNMP with support for authentication, access control and privacy.
Subnet	A group of networked computers that all share a common IP address prefix. All devices within the same IP subnet can be reached in one hop without a router.
Subnet mask	The IP decimal representation for the subnet prefix of the IP address. The subnet mask specifies the length of the shared subnet prefix as used by all devices in the local subnet. A subnet mask of *255.255.255.255* is used by the Ethernet switch to isolate a specific IP address.
Switch	A device that connects several LANs together to form one logical LAN. A switch is similar to a bridge, but usually offers more sophisticated features for bridging LANs of different types.
TFTP (Trivial File Transfer Protocol)	A simplified version of the TCP/IP file transfer protocol used by the switch to transfer saved configuration profiles and to perform new firmware updates. The switch can download new firmware from a customer's TFTP server. A username and password are not required by the TFTP protocol.
VLAN (Virtual Local Area Network)	A logical subgroup which acts like a LAN and communicates as if attached to one broadcast domain.

Index

Pushing Performance

HARTING Technology Group
info@HARTING.com
www.HARTING.com

Version vom 10. 2013