



People | Power | Partnership

HARTING Ha-VIS Management Software mCon 3000 Next Generation

User Manual Web Interface

All brand and product names are trademarks or registered trademarks of the owner concerned.

3rd Edition 2013, revised 10/13

© HARTING Electric GmbH & Co. KG, Espelkamp

Author: HARTING Scriptor Dokumentations Service GmbH Editor: HARTING

All rights reserved, including those of the translation.

No part of this manual may be reproduced in any form (print, photocopy, microfilm or any other process), processed, duplicated or distributed by means of electronic systems without the written permission of HARTING Electric GmbH & Co. KG, Espelkamp.

Subject to alterations without notice.

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



Content

1.	Introduction					
2.	Safety Guidelines and Approved Usage					
3.	General Notes about this Manual	9				
•••	3.1 Explanation of the symbols	9				
	3.2 Typographical conventions	9				
	3.3 Additional information	9				
4.	Basic Operation					
	4.1 Switch access and configuration					
	4.2 Web access					
	4.3 SNMP configuration	11				
5.	Multifunction Button					
6.	Introduction to the Web Browser Interface					
	6.1 The menus					
	6.2 Accept and saving changes with the Save Configuration button6.3 User rights	14 16				
7.	Overview					
8.	System Settings	19				
	8.1 General Settings and Switch Management					
	8.2 Port Settings	21				
	8.3 User Management	23				
	8.4 SNMP	25				
	8.5 Network Discovery					
	8.6 Time Settings					
	8.7 DHCP Relay Agent8.8 File Transfer					
9.	PROFINET					
10	Redundancy	40				
	10.1 RSTP	40 40				
	10.2 MRP					
11.	VLAN					
	11.1 Basic Settings					
	11.2 Port Settings	48				
	11.3 Static VLAN					
12.	Quality of Service					
	12.1 Basic Settings	51				
	12.2 802.1p Priority Mapping	51				

13.1 14.1 14.3 15 1 15.2 15.3 15.6 16.1 17.3 18 1 18.2 Appendix



Figures

Figure 4-1	General Settings
Figure 5-1	Operating the Multifunction Button
Figure 6-1	Screen structure
Figure 6-2	The menu tree
Figure 6-3	Save Configuration button
Figure 6-4	Invalid entry: The exclamation point indicate
Figure 7-1	The Overview section
Figure 8-1	General Settings window
Figure 8-2	Switch Management window
Figure 8-3	Basic Settings tab
Figure 8-4	Port Control tab
Figure 8-5	User Management tab
Figure 8-6	Change Password tab
Figure 8-7	SNMP section
Figure 8-8	LLDP Settings tab (Network Discovery secti
Figure 8-9	LLDP Connections (Network Discovery sect
Figure 8-10	Advanced LLDP Settings (Network Discove
Figure 8-11	Time Settings window
Figure 8-12	PTP Settings section
Figure 8-13	DHCP Relay Agent tab
Figure 8-14	Import/Export Firmware tab
Figure 8-15	Save/Load Configuration tab
Figure 8-16	Reboot tab
Figure 9-1	PROFINET window
Figure 9-2	IP settings in PROFINET Profile
Figure 9-3	LLDP settings for PROFINET
Figure 10-1	Basic Settings tab
Figure 10-2	Port Settings tab
Figure 10-3	RSTP Port Status tab
Figure 10-4	MRP Domain Settings with invalid SD card.
Figure 10-5	MRP Domain settings with a valid SD card.
Figure 10-6	MRP Domain - Basic Settings
Figure 10-7	MRP Domain Status window
Figure 11-1	VLAN Basic Settings tab
Figure 11-2	VLAN Port Settings tab
Figure 11-3	Static VLAN Configuration tab
Figure 12-1	Quality of Service – Tag Control Information
Figure 12-2	QoS Basic Settings
Figure 12-3	802.1p Priority Mapping tab
Figure 12-4	DiffServ Priority Mapping tab
Figure 12-5	Rate Limiting
Figure 13-1	IP Authorized Manager
Figure 13-2	802.1x Basic Settings tab
Figure 13-3	Port Settings tab
Figure 13-4	Local Server tab

Content

	11
	12
	13
	14
	14
s an improperly formatted IP address	15
	17
	19
	20
	21
	22
	23
	20
	24
n)	22 مر
ווע	20
OII)	29
y section)	30
	30
	32
	33
	34
	36
	37
	38
	38
	39
	40
	42
	43
	44
	44
	45
	46
	47
	49
	50
(101)	50
	51 51
	51 52
	52
	53
	54
	55
	56
	57



Figure 13-5	Radius Server Configuration tab	57
Figure 13-6	Supplicant Session Info tab	58
Figure 13-7	Timers tab	59
Figure 14-1	Link Aggregation Basic Settings tab	61
Figure 14-2	Link Aggregation Interface Settings tab	62
Figure 14-3	Link Aggregation Port Settings tab	63
Figure 15-1	IGMP Snooping Basic Settings tab	65
Figure 15-2	IGMP Timer tab	66
Figure 15-3	IGMP Snooping VLAN Configuration tab	67
Figure 15-4	IGMP Snooping VLAN Router Ports tab	68
Figure 15-5	IGMP Snooping VLAN Multicast Group tab	68
Figure 16-1	E-mail Alarm tab	69
Figure 16-2	SMTP Server Settings tab	70
Figure 16-3	SNMP Trap section	70
Figure 17-1	Ingress Statistics tab	71
Figure 17-2	Egress Statistics tab	72
Figure 17-3	Histogram tab	74
Figure 17-4	Port Mirroring section	75
Figure 17-5	Switch History event list	76
Figure 17-6	MAC Address Table	78
Figure 17-7	Light Beacon functionality	79
Figure 17-8	Ping functionality	79
Figure 18-1	Interface Statistics tab	80
Figure 18-2	Ethernet Statistics tab	81
Figure 18-3	RSTP Information tab	82
Figure 18-4	RSTP Port Statistics tab	82
Figure 18-5	IGS Statistics tab	83
Figure 18-6	IGS V3 Statistics tab	83
Figure 19-1	Slot for SD card on the backside of the switch	84
Figure 20-1	Installing the GSD file	86
Figure 20-2	Select GSD file	87
Figure 20-3	Component library	87
Figure 20-4	Adding a switch	
Figure 20-5	System characteristics	
Figure 20-6	Assign Device Name	
Figure 20-7	Select the switch and assign the names	
Figure 20-8	Slots and modules of the Ha-VIS mCon 3000 Next Generation switches	
Figure 20-9	Alarms on Slot 0	90
Figure 20-10	Topology settings	91
Figure 20-11	Transmission medium / duplex settings	91
Figure 20-12	Port-related alarms	92
Figure 20-13	QoS settings	92



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 Appendix	Information about SD Memory Card and other service 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.



3.1 Explanation of the symbols

The following symbols are used in this software guide:



-25

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

damage to property may result.

Note

this manual.

3.2 Typographical conventions

This manua	l uses	the	following	typ
------------	--------	-----	-----------	-----

14 - 12	Tau di in
Italics	lext in
	down li
	menu (
	list cho
Bold	Text in
	the so
	display

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.

at http://www.HARTING.com.

General Notes about this Manual

This word describes warning notes that indicate a low-level source of danger. If not avoided,

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

ographical conventions to describe the software interface:

italic font refers to an entered value, a selection from a droplist (such as Enable), a reference to a section of the software (such as System Settings \rightarrow General Settings) or drop-down pices.

bold font refers to the name of a row or column found within ftware interface, or to the name of a field where data is yed or specified.

The latest versions of the switch firmware and the manual can be downloaded from the Internet

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.

- HTTP connection to the switch.



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.

Basic Operation

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

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.



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,	Set the switch to factory default settings with the exception of the IP
	keep 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.

👫 Support 🚯 About							Seaston Timecut: 1958.63 🚡 admin 😡 Legout
HARTING Parking Parlowman		A					HARTING Technology Group
-	1 <u> </u>						Overview
mcm3902-aastp	OVERVIE	W					
them since							
E System Settings		Device Name: mcm2002-0	ctass				
PROFILET		Device Cartacl: HARTENGE	28				
E Robindancy		Device Locations					and all all all all all all all all all al
VLAN		Device Description: He-VIS-reCo	n 31.02-AASFF 23751124300				a catter of
≥ 0o5		Fart-fax - 207511243	08				
E Socialty		Hardware Huston: 1975.5					18
Lak Aggregation		naranara tasan Pasa		_			38
- Multicatt		Pethologia Verboni: 2.5.5		C			100
S Alarm		Webcl Version: 3.3.3		U			
		Fort Count: 13					
		IP-Addwort 182168.03	200				
		NAC-Address: 02:31 PC 0	6A 20 8				45
		Device Up Tree: 0Darrs, 16/	Hours, 17 Mondes, 19 Second	in in the second se			
	Part	Jack Type	Status	Lask	Automophistion	Data Rate	Duplex Mode
	1	510	Enable		On	1GR()r	FullDuplex
	2	579	Enable		ón	1000.3	Hell Dugles
	2	136	Enable		on	100Milety/v	FullDapley
		8365	Fraik		05	scenals	Hell Dugler:
	5	P.W.	India		05	100000	ting to play
		8345	E-AL			10-04-	the basis
		1045	Drate		01	10-005	THE DIGHT
	7	1045	0.406	•	05	10464/s	Half Digler:
	0	1045	Enable	•	On	10/065	Hall Duckex
		R345	Enable	•	on	300M840/2	Pul Daplex
	20	RONS	Enable	•	On	10404/2	Helf Duplex
					D		
P.Acd esc 152 588.5.248 5a5	aret March: 215,255,255	LE MACAGERS MITTERED	PAR Permanet 3.5.5				Save Coeffy
		E ¹ O f	•				
		⊢igure 6-1	Screel	า structure	;		

The top task bar	
The second tax s	

- в The menu tree
- С The active window
- The bottom task bar D

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.

Α

Introduction to the Web Browser Interface

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.

HARTING	Pushing Performance	1
mcon3102	aastp	
Overview		
E System S	ettings	
PROFINET		
Redunda	ку	
VLAN		
⊕ QoS		
Security		
Link Agg	regation	
Multicast		
Alarm		
🗄 Diagnosti	¢	
(ii) Continuing		

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.

Configuration is not saved persistant: 😹 Save Config

Save Configuration button Figure 6-3



Assuming configuration changes and permanently saving them

- button.
- 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

-2

6.3

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.



General Settings

Device Name:
Device Contact:
Device Location:
IP Address Mode:
IP Address Alloc Protocol:
IP Address:
Subnet Mask:
Switch Base MAC Address:
Default VLAN Identifier:
Configuration Save Status:
Remote Save Status:
Configuration Restore Status:
Http Port Number:
d data required!
Apply

Figure 6-4

HARTING Electric GmbH

Introduction to the Web Browser Interface

The software maintains any configuration changes in volatile memory after pressing the Apply

· The administrator must explicitly trigger the save operation (bottom bar after changing

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.

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 <i>Guest</i> enables all areas of the software to be viewed only.
Admin	The access category <i>Admin</i> 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.

ARTING

HARTIN

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.

Overview window:

OVERVIEW			
	Device Namer 1	started and a	
	Device Contact: 1	WEITENS CON	
	Device Cocations		
	Device Decorptions IN	series inclusion 3142-44599-2426	4.124000
	Patric: 1	875112×308	
	Firmer Resident	15.5	
	web.Ethnion 1	1.3.3	
	Fort Count:	10	
	IP-Address I	52.84.1280	
	Device Up Timer 1	10es, 94 Hors, 57 Minutes, 1	19 Seconds
Red.	Jurk June	(Labor	144
1	39	Dalle	
2	32	Enable	
3	126	trade	•
•	8345	Evalue Date	:
	106	Enable	
,	RME	Diable	
	104	Dable	
9	626	Crable Crable	
Function	on		Descrip
. .			
Device	Name		Displays Default
Device	Conta	rt.	Display
201100	oomu		Setting
Device	Locati	on	Displays
			Genera
Device	_	ntion	
	Descri		MACac
	Descri	puon	MAC ac
Part No	o. Descri	ption	MAC ac Displays
Part No Hardwa	e Descri o. are Vers	sion	MAC ac Displays Displays
Part No Hardw	e Descri o. are Vers	sion	MAC ac Displays Displays
Part No Hardwa	e Descri o. are Vers	sion	MAC ac Displays Displays board.
Part No Hardw Firmwa	e Descri o. are Vers are Vers	sion	MAC ac Displays Displays board. Displays
Part No Hardwa Firmwa	e Descri o. are Vers are Vers	sion	MAC ac Displays Displays board. Displays
Firmwa WebUl	e Descri o. are Vers are Vers	sion sion n	MAC ac Displays Displays board. Displays

Port Count IP-Address MAC-Address **Device Up Time**

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



on

ption

s the type of HARTING Ethernet switch in use.

Ha-VIS mCon 3080-A, Ha-VIS mCon 3102-AASFP value: ys contact information, as defined by the user in the General section.

ys the location of the device, as defined by the user in the al Settings section.

ddress of the switch

ys the HARTING part number of the switch.

s the hardware version number of the switch management

ys the firmware version number of the switch.

ys the version of the web interface.

Displays the number of ports.

Displays the currently assigned IP address on the switch.

Displays the unique hardware MAC address on the switch.

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 \rightarrow Port Settings menu section.

Function	Description
Port	Displays all available switch ports.
Jack Type	Displays the compatible media or jack type for the port (<i>RJ45</i> , or <i>SFP</i>).
Status	Displays the current status of the port. <i>Enable</i> means that the port is enabled; <i>Disable</i> is displayed if the port is disabled. (A port can be disabled in the <i>System Settings</i> \rightarrow <i>Port Settings</i> 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. <i>Half duplex</i> means that data flows in one direction via the port at a given time; <i>Full duplex</i> 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.

Device Nerve:	rcm2132-earlp	
Device Carked:	HARTING LOPH	
Device Location:		
IP Address Mode:	Marsai	
Philosoffication Polacil.	5102	
DHO ¹ Feet Access	Divelvie	
IP Address	181-168-0-200	Seve P Abbert I
Subnet Mark	299-299-299-4	
Default Catemay:	0.0.0.0	
Satch Base MAC Address:	00.11 / 10.02 40	
Default VLAN Menther:	1	
Configuration Solve Status:	Not Invitated	
Configuration Export Status:	fect instand	
Configuration Review/Support Status:	Successful	
HTTP Part Runders	00	
held fields are required.		

Figure 8-1

The following general settings can be displayed or specified:

Function	Descri
Device Name	Specify
Device Contact	Specify
Device Location	Specify
IP Address Mode	Specify the dro and su If <i>Man</i> e
DHCP Fast Access	The fu The si minimu 82 is u
IP Address	Specify automa
Note	

3

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.

System Settings



General Settings window

ription

fy a descriptive text for the device name.

fy a descriptive text for the device contact.

fy a descriptive text for the device location.

fy the switch IP addressing mode. If Dynamic is selected in op-down list, the switch is assigned with a valid IP address ubnet mask during system initialisation by the DHCP server. nual is selected, the IP address and the subnet mask must be ed manually.

unction accelerates the DHCP addressing in large networks. standard timeouts and waiting periods are reduced to a um. It is recommended to set this option to enable, if Option used.

fy the IP address of the switch. IP addresses are assigned atically if a DHCP server is activated.

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.

Switch Management				
Websessian				
web bears Treeput (res): 690	2			
Paceve lamber of intel scenere 2				
Management				
Defail/Meagenet-VLHUD: 8		(the setting will only take effect after a restart)		
HTP-Put: 00		(the setting will take offset inmediately ()		
Malifurction Bullions Enal	die) w			
Annaly				

Figure 8-2 Switch Management window

Web Session

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

Management

Function	Descri
Default/Mgmt-VLAN	Change
ID:	Range
	Defaul
HTTP Port	Sets th
	Range
	Default
Multifunction Button	Enable
	Range
	Defaul

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

				Basic Settings	Port Control
ortBa	sic Settings				
Port	t i	Admin State	Link Status		
1		Up 🖃	•		
2		up 🖃	•		
3		up 🖃	•		
4		Up 🖬	٥		
5		Up 🖃	٥		
6		up 🗉	0		
7		up 🖬	0		
8		up 🖃	•		
9		up 🖃			
10		Up 🖃	•		

Figure 8-3 Bas	sic Settings tab
----------------	------------------

In this tabbed section, the administ has the following columns.

Function	Descrip
Select/Port	Select
	checkbo
Admin State	Select t
	or disat
	Range
	Default
Link Status	Display
	device i
	is conne

System Settings

ption

je of the Management VLAN
e of value: 1 ... 4094
it value: 1
ine http port for the web interface.
e of value: 1 ... 65535
it value: 80
e or disable the Multifunction Button on the switch
e of value: Enable / Disable
it value: Enable

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

ption

the port that you would like to change by clicking on the ox here.

the desired state of the port. A port can be either enabled (up) bled (down).

of value: UP / DOWN

t value: UP

ys the port status. A green circle in this column indicates that a is connected to this port. A red circle indicates that no device nected.

8.2.2 Port Control

Part	Autone patistion	Daplex	Speed	How Control Admin Status	Autocressing
1	Today of	Pall x		Dualle w	Adv +
2	0.00	Hat we	PG002941 44	Double M	A.00 - 4
9	that is	Pull ~	DOIMDR/AND M	Dualle m	Adv m
4	Doble (m)	Hall w		Divatile se	Adv m
3 8	shill in	Half 4		Dealle M	A/0 m
6	findle (w)	16.87 vr		Dualde w	Adv w
2	Under w	108		Double M	Ada m
	truble (w)	Hall w	acebetos: w	Dealle M	A/0 (m)
9	Code (e)	Pull w.		Divalle w	A.fu m
3.80	chable (m)	1620		Deadle M	Add m

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 checkbox here.	at you would like to change by clicking on the
Autonegotiation	Select whether Autor is a function which of determine the best negotiation function (<i>Disable</i>). If <i>Enable</i> is and the data-rate ar Range of value: Default value:	onegotiation is disabled or enabled. Autonegotiation enables the participating interfaces to automatically st possible transmission parameters. The auto- in can either be activated (<i>Enable</i>) or deactivated is selected, the auto-negotiated settings will be used and duplex columns will be greyed out. <i>Enable / Disable</i> <i>Enable</i>
Duplex	Select the data trans down list. <i>Half</i> mean a given time; <i>Full</i> en Range of value: Default value:	smission mode for the respective port from the drop- ns that data flows in only one direction via the port at ables data to flow in both directions simultaneously. <i>Half Full</i> <i>Full</i>
Speed	Select the data tra list: 100 Mbit/s or 1 type of port interfac Range of value: Default value:	nsmission rates for the port from the drop-down 0 Mbit/s, 100 Mbit/s or 1 Gbit/s, depending on the ce. 10 Mbit/s or 100 Mbit/s / 100 Mbit/s or 1 Gbit/s Physical maximum
Flow Control Admin Status	Select if flow control is activated (<i>Enable</i>) or deactivated (<i>Disable</i>). If enabled, the port sends out Pause frames when the buffer capacity reaches a certain limit. Range of value: <i>Enable / Disable</i> Default value: <i>Disable</i>	
Autocrossing	The automatic cross standard auto mode MDIX (RX / TX lines Range of value: Default value:	sover of the RX / TX lines can be switched from the e in the following modes: MDI (no crossing of lines), s are crossed) and AUTO (automatic crossover). MDI / MDIX / AUTO 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.



HARTIN

8.3 User Management

account.

8.3.1 User Management

Basic Information			
Total Number of Overse	2		
Currently Logged On Users:	1		
Create User			
Usernome:			
Level	Guest	(m)	
Password			(nin, 6 cheracters rec
Rotype-Password			
Bald fields are required.			
Greate			
User List			
thername			
adhir (current unir)			
guest			
Apply Dobris			

Figure 8-5	User Managemen
Create User	To cr admir After
User List	must be ve All us
	of us switc

3

System Settings

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



nt tab

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

sers existing on the switch are shown in this list. The maximum sers is limited to 20. Selected users can be deleted from the ch 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

			User Management	Change Password	
hange Password					
Current User:	admin				
Current User Password:					
Users:	adnin 💌	1			
New Password:		(nin. 6 characters required!)			
Retype-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.

SNMP V1/V2C	
🔽 Enable	
Read Community:	public
Read/Write Community:	private
Bold fields are required.	
Apply	
SNMP V3	
F Enable	
Username:	harting
Access Level:	AuthPriv
Authenticaton Protocol:	MD5
Authentication Password:	
Authentication Retype-Password:	
Privacy Protocol:	DES
Privacy Password:	
Privacy Retype-Password:	
Bold fields are required.	
Apply	

System Settings





HARTIN

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 switch via SNMP v Range of value: Default value:	launch the SNMP agent and allow access to the ersion 1/2c. Enable / Disable Enable
Read Community	Specify the commu public. Range of value: Default value:	Not more than 20 printable characters.
Read/Write Community	Specify the community name for SNMP read and write access. The default is <i>private</i> . This community string acts as an SNMP passwork you should pick one that it difficult to guess. Range of value: Not more than 20 printable characters Default value: <i>private</i>	

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 r	name for SNMP version 3 access.	
	Range of value:	Not more than 20 printable characters.	
	Default value:	harting	
Access Level	NoAuthNoPriv AuthNoPriv	No authentication and no message encryption 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	Desci
Authentication	Protoc
Protocol	Algori
	Rang
	Defau
Authentication	Speci
	Rang
	Defau
Authentication Retype Password	Repea
Privacy Protocol	Protoc
-	Range
	Defau
Privacy Password	Specit
	Range
	Defau

Privacy Retype Password

Note

If you don't plan to use SNMP, yo maximum security is ensured.



 $\overline{\mathbf{a}}$

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.

System Settings

 Description

 Protocol used for User Authentication (MD5) or Secure Hash

 Algorithm (SHA)

 Range of value:
 MD5 / SHA

 Default value:
 MD5

 Specify the SNMPv3 password. It must be at least eight characters.

 Range of value:
 Not more than 20 printable characters

 Default value:
 none

 Repeat the specified SNMPv3 password.

Protocol used for privacy. **Range of value:** *DES* **Default value:** *DES* Specify the SNMPv3 privacy password. **Range of value:** Not more than 20 printable characters **Default value:** none Repeat the specified SNMPv3 privacy password.

If you don't plan to use SNMP, you should make sure that both versions are disabled so that

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

						CLOP Set	ungs	eter connectoris	
DP	Settings								
		Activate LLDP:	R						
		Chassis ID Subtype:	Mac Address						
		Chassis ID:	00:11:fc:00:d4	:0					
		Transmit Interval:	30 (default)	-					
		TTL Multiplier:	4 (default)	-					
		Send IP Address:	R.						
F	Port	Port ID Subt	ype		Port ID				
E :	1	If Alas	-		Skot0/1				
E 2	2	If Alas	-		Skot0/2				
	3	1f Alas	-		Slot3/3				
E 4	4	1f Alias	-		Slot0/4				
E 1	5	If Alias			Slot2/S				
□ €	6	If Alas	-		Skot0/6				
Г 7	7	If Alas			Slott)/7				
-		If Alas	-		Slot0/8				
1.1		If Alas	-		Skot0/9				
E 9	9								

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

Note

-25

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

8.5.2 LLDP Connections

LDP Connections			
Local Pert	Neighbour Chasain ID	Neighbour Port 30	Neighbour IP
1	statence = 300-2	port-009	296.236.0.192
•	ncav0080-a	pari-009	192

Figure 8-9 LLDP Conne

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
- Neighbour Chassis ID
- Neighbour Port ID
- Neighbour IP

LLDP Connections (Network Discovery section)

- Local port where the information was learned
- $\label{eq:chassis} \mbox{ID of the neighbour device}$
- Port ID of the neighbour device
- IP address of the neighbour device

8.5.3 Advanced LLDP Settings

	and a second a	COP COMEDOMS	Advanced LLOP Settings	_ C
Port coeffig				
To and Ro (m)				
To walks (m)				
Tx and Rx (m)				
To and the law.				
To and its (m)				
Tx and Rx (m)				
Tradity in				
To and its (m)				
To and Ro Inc.				
To and Ro (w)				
	Pert config Tri addite inc Tri addite inc	Pert coolig Traditio Ne Traditio Ne Traditio Ne Traditio Ne Traditio Ne Traditio Ne Traditio Ne Traditio Ne Traditio Ne Traditio Ne	Port config Tradito m Tradito m Tradito m Tradito m Tradito m Tradito m Tradito m Tradito m Tradito m	Peri ceelig Tradito := Tradito := Tradito := Tradito := Tradito := Tradito := Tradito := Tradito := Tradito := Tradito :=

Fiaure 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 fr on a specific port.			
	Range of value: Default value:	Tx only / Rx only / Tx and Rx / Disable 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

								Time Settings	PIP	۲
Time Settings										
Bosic Time Settings										
Current Time Sources	#7C									
Manual Time Settings										
	New Yolke	General	ul.w							
Text	60 06 32	00.06.32								
Date:	88 - 88 - 297	0.015	70							
	det Tier(HTC)									
Automatic Time Settings										
Advigides	R									
284	Not Sundronand									
Section 2010	64	(64-15291)								
Treore	+82.00	(Pamator/)H	676							
Primary ShiP Server IP:	192.968.0.1									
Secondary 2022 Server 3P										
Bald fields are required.										
Apply										





Manual Time settings

Function	Descrip
Current Time Source	RTC/PT
Time	Specify displaye (24-hou <i>Value</i> co
Date	Specify below C specifie
Get Time	Click on into the

Automatic Time settings

Function	Descr
Auto Update	Check
	the su
Status	Shows
Interval	Specif
	update
	Range
	Defau
Time Zone	Specif
SNTP Servers	Specif
	time. T
	specifi
	addres
	to prov

Note

2

starts with the following system settings after booting up: Time 00:00:01

Date 01-01-1970

logged.

8.6.2 Precision Time Protocol (PTP)

determined using the "best master clock" algorithm.

tion

P/NTP

- the system time manually. The current system time is ed below Current Value in the format hours:minutes:seconds format). The time can be specified manually in the New olumn.
- the date manually. The currently set date is displayed *Current Value* in the format day-month-year. The date can be d manually in the New Value column.
- this button to enter the computer system's time and date fields above. The time information will be taken from the computer on which the web browser is running.

ription

- this box in order to receive the system time automatically with pport of a SNTP server.
- s the current synchronization status
- ify the period of time in minutes. The system time is then ed periodically at this interval.
- e of value: 64 16284
- ilt value: 64
- ify the Time Zone -12:00 ... + 12:00
- ify the address of the SNTP servers that will supply the system The address can be that of either a publicly-accessible PC or a ied PC in the network that serves as a time generator. The IP ss must be specified. More than one server may be specified vide redundancy.
- The Ethernet switch stores time and date up to 72 hours after power off. By default, the switch
- 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

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

HARTIN

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.
- ٠ 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.

		Texa Lottings	10	0
PTP Settings				
Beac PIP Configurations				
Create PTP:				
PTP Modes	Bashy w			
PTP Peorty G				
PTP PAGE 20				
Two Step Hode				
Two Step Temperant Cacle				
Delay-Hochanism Transparant-Cocks	Excluded w			
PTP Status				
Graduate Mettys				

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: 0255
	Default value: 0
PTP Priority 2	Enter the priority 2. Available only in boundary mode
	Range of value: 0255
	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-	Define whether the switch device should send only Sync-Messages
Clock	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	Specify the delay mechanism of the transparent clock. (Transparent
Transparent-Clock	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.

itself.

DHCP Relay Agent		
DHCP Relay Agen	t Status: Disable	-
DHCP O	ption 82: Disable	
0	rcuit-ID: Vand	ID Fort ID
Re	mote ID: C Defa.	Jt C Device Nam
DHCP Server Remotel	ID Entry:	
	Port	Circ
	1	
	2	
	3	
	4	
	5	
	6	
	7	
	8	
	9	
	10	
Bold fields are required.		
Apply		
DHCP Server - Add		
DHG	Server:	
Bold fields are required.		
DHCP Server - List		
Server Address		
Delete		
Figure 8-13	DHCP Re	lay Agent
Function		Descri
DHCP Relay A	gent	Enable
Status	•	Ontion
Juluo		Dance
		Range
		Defaul
DHCP Option 8	32	Select
		Range

Circuit-ID

es or disables the DHCP Relay Agent on the switch. To use 82 this option must set to enable. of value: Enable / Disable / Enable RFC conform It value: Disable whether to disable or enable Option 82 on the switch. of value: Enable / Disable Default value: Disable Defines the Circuit-ID to identify the location of the end device in the network.

System Settings

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

	DHCP Relay Agent	•
e IP Address II Custon		
suit-ID		
tab		

iption

Range of value: VLAN ID / Port ID



RTING

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 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	Descr
TFTP Server	Specif
File Name	Specif

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.

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	Enter calculated value of the Remote ID. If the Remote ID is used			
RemoteID Entry	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.

		Fitment .	Configuration	DBOX.	0
TFTP Transfer					
Correct fermane package:	HTS_JTCH40016006_015_50005.1er.pr				
10'10' Server:	8108				
File Norme:	vers preserver, and (Vie extension must be tax.gr.)				
Expert Tarafer Status	Ref Dilated				
Equit have Salar	Ref Dilated				
multifields are required.					
Japort Expert					
HTTP Transfer					
File Import	Dathaten, Neier Sold as				
Therafer Status	Ret Instead				
Build fields are required.					
Saport Report					
Note:					
Venuel rebort to required after feministra in	port.				

Figure 8-14 Import/Export Firmware tab





System Settings

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

ription

fy the IP address of the TFTP server

fy the file name of the configuration

8.8.2 Configuration

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

		Personal I	Configuration	Petert	(\mathbf{F})
Configuration Settings					
Load Type:	Load Centre on Hanhar Int				
Configuration Save Status	lot intered				
Bald Feith are required.					
Amh					
TFTP Transfer					
File Name:	his participan cud				
TPTP Server	8808				
Configuration Separat Status	RLR 1 Vilated				
Configuration Export Status	Ruit Divisioned				
Beld Feits are required.					
Japat Equat					
HTTP Transfer					
Pile Suport:	Dashachen. Keine Detei aus				
Beld fields are recurred.					
Japat Equat					
Note:					
Palastic required after restarcing of	L				

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: <i>hss_config_files.cpak</i>
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.

command.

System Settings

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



9. PROFINET

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

	Profinet Settings	0
tOFINET Settings		
moreen p		
PROPINET Rank Stratus Tandied		
UEP Statum Dadded		
M feids are required.		
Apply		
tD Export		
Centrel (GD File: 020%-13_1498/ThG-MC042000-8-5MT04-20120927) ar gt		
Expert		



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.



IP settings in PROFINET Profile Figure 9-2

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.



-2

HARTIN

controller.

Note

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

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.

Settings are not	aged by PROFIL	ET Das	at .		
	ADVER LEPT				
0	ent D fuitper				
	Chanada Tat		100.44		
1 and	(m) local (m)				
	TL Hulphro				
Part	Port	10.54	Mape		
1					
2	Cut				
3	Cut				
4					
5					
8	Out	lon.			
7					
8					
9	Cut				
10					

Figure 9-3

PROFINE

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

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



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.

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

Note

							Basic Settings Port Settings	Port Status
RSTP Basic 5	Settings							
Status	Version	Priority	Hax Apr (sec)	Hello Time (sec)	Tx Hold Count	Forward Delay (sec)	Dynamic Path Cost Calculatio	
Endled m	RSTP Conparible	32768 .	20	2	6	18	The m	
Andr								
To set the parameter 2 x (Forward Delay	Forward Celley' & Wax.Apr' the follow - 1) Im Max.Apr	wing relation is to be satisf	wi.					
To set the parameter Max Age >> 2 x the	Yelo Time' & Vax Ape' the following the Time + 10	relation is to be satisfied.						

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 switch. Range of value Default value:
Version	Select the prote Range of value Default value:
Priority	Specify the STR tree. The bridg root. A higher priority is 0. The Range of value Default value :
Max Age	Specify the time received in a R Range of value Default value:
Hello Time	Specify the time BPDUs. Range of value Default value:
Tx Hold Count	Specify the masecond. Range of value: Default value:
Forward Delay	Specify the per learn period) be Range of valu Default value:
Dynamic Path Cost Calculation	Select whether calculation is a will be calculate Range of value Default value:
Note	
It is recommended to case of a link failure.	use RSTP inst



-2

Note

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 >= $2 \times (\text{Hello Time} + 1)$

to disable or enable a global redundancy protocol on the

ie: Enable / Disable Enable tocol version. **Je:** RSTP Compatible / STP Compatible **RSTP** Compatible

P priority. This is used to identify the root bridge in a spanning ge with the lowest value has the highest priority and is the numerical value means a lower priority; thus, the highest ne highest numerical value on the drop-down list is 61 440. ue: 0 ... 61 440 in steps of 4096

32 768

he in seconds (STP) or hop count (RSTP) that the information STP BPDU (bridge protocol data unit) is valid.

Je: 6 ... 40

20

ne interval in seconds between two successive configuration

le: 1 ... 2 sec 2 sec

naximum number of BPDUs that can be transmitted in a

Je: 1 ... 10 6

riod of time in seconds that a bridge will wait (the listen and before beginning to forward data packets.

Je: 4 ... 30 sec

15 sec

the dynamic path cost calculation is allowed or not. Cost allowed when this is set to *True*, the pathcost of all the ports ted dynamically based on the speed of the interface.

ie: True / False True

tead of STP to reduce the time for the network recovery in

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

10.1.2 Port Settings

Part	Fale	Peketty	RSTP Status	Puth Cost	Protocol Higration	Admin bdge Part	Admin Point To Point	Auto Edge Detection	Restricted Role	Resident TON
1	Designated	120 m	Enabled of	23000	alimit	False int	Ada M	True (m)	False M	False M
z	Disabled	128 M	shadied (m)	2300000	Mort.	Pale (m)	Age (m)	748 [8]	Paine [m]	Paire [m]
3	Roat	128 W	Ended w	230000	Stat	False at	Auto w	That at	False or	Fairs an
	Doddind	120 M	Enabled or	2300000	Start	False or	Ada m	Team and	Faire or	False M
5	Disabled	128	tradied int	2300000	Mark	Faire int.	Ada (H)	740 .00	Paine (m)	Pala (m)
4	Dualed	128 M	Enabled w	23000000	52 mil	Faire an	Ada w	744 14	Faire int	Fair at
7	Diskind	120 m	Enabled at	2300000	- start	Faire an	Ada M	Top or	False or	False w
	Deabled	120 M	Enabled (m)	2300000	Stort.	False int	Ada M	True and	Faire int	False M
	Designated	120 M	Enabled (m)	230000	staat .	Page (m)	Inda (m)	310 M	Palan (m)	Palas (m)
10	Dealer	125 m	Evabled m	23000000	- Mart	False at	Adv W	True (m)	False and	False and

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 <i>Enabled</i> or <i>Disabled</i> to enable or disable RSTP for the corresponding port. Range of value: <i>Enable / Disable</i> Default value: <i>Enable</i>
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 2,000,000 1 Gbit/s 20,000 Range of value: 0 200,000,000
Protocol Migration	When operating in RSTP mode, pressing the <i>Start</i> -Button forces this port to transmit RSTP BPDUs.
AdminEdge Port	Select <i>True</i> if the port is acting as an edge port. Range of value: <i>True False</i> Default value: <i>False</i>
Admin Point to Point	Select the <i>Force True</i> option to configure a port as point-to-point. The port can be forced to a non-point-to-point state by selecting <i>Force False</i> . If you select <i>Auto</i> , the decision is made dynamically. Range of value: Force True / Force False / Auto Default value: Auto



HARTIN

Function	Description
Auto Edge Detection	Select <i>True</i> dynamically. Range of va Default valu
Restricted Role	Select the re restricted so can be selec A <i>True</i> setting Range of va Default valu
Restricted TCN	Select the r the port. If s change notif the topology Range of va Default value

10.1.3 Port Status

Dave B	Decise sted Reet	Designated Cost	Decise stad Bridge	Design steel Best	Turne	Bole	Bast Et al.o
POR	Designaced Rook	Designaced Cost	Designaced bridge	Designaced Port	type	Rose	Port state
1	40:00:00:90:e8:19:bc:60	0	40:00:00:90:e8:19:bc:60	80:08	Point-to-Point	Root	Forwarding
2	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	Shared LAN	Disabled	Blocking
3	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	Shared LAN	Disabled	Blocking
4	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	Shared LAN	Disabled	Blocking
5	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	Shared LAN	Disabled	Blocking
6	40:00:00:90:e0:19.bc:60	200000	00:00:00:11:fc:00:f4:60	00:06	Point-to-Point	Designated	Forwarding
7	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	Shared LAN	Disabled	Blocking
0	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	Shared LAN	Disabled	Blocking
9	00.00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	Shared LAN	Disabled	Blocking
10	00-00-00-00-00-00-00	0	00:00:00:00:00:00:00:00	00:00	Shared LAN	Disabled	Blocking

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 bridge record
Designated Cost	Displays the to this port.
Designated Bridge	Displays the This is the pro- bridge for its s
Designated Port	Displays the segment.
Туре	Displays the This indicate connection or
	Function Designated Root Designated Cost Designated Bridge Designated Port

if you want to have the edge port status calculated

alue: True / False

le: True

restricted role status of the port. If set to True, the port is that it may not be selected as a root port. A restricted port cted as an alternate port after the root port has been chosen. ng can result in poor connectivity within the spanning tree.

alue: True / False

False le:

restricted TCN (Topology Change Notification) status of set to True, the port does not propagate received topology fications or topology changes to other ports. This prevents change is caused by that port.

alue: True / False False ue:

unique bridge identifier (Priority + MAC address) of the led as the root for the segment to which the port is attached. path cost of the designated port to the segment connected

designated bridge identifier (MAC address) of the bridge. referred bridge which this port considers as the designated segment.

number of the port on the designated bridge for this port's

operation status of the LAN segment attached to this port. es whether a port is considered to have a point-to-point r 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 (<i>Forwarding</i> , <i>Blocking</i> , <i>Disabled</i> or <i>Learning</i>) 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:

		HARTING Technology Grou
		/ Baile Sattings / 1997 Status / 🕐
MRP Domain Settin	ngs	
Note:		
No 50-Card Inserted Plea	ee levert a 50-Card with MIP expandity and rebect to mable MIP.	

Figure 10-4 MRP Domain Settings with invalid SD card

With a valid SD card following page appears:

Realized Parlowners								PARI	ING Techn	orogy c
	I								Rain Settings	MEP Dates
n1102 arelp	MRP Domain Settings									
ine w										
stens Settings	Domain Rules	Hanape	(M)							
Conce of Settings	Damain ID	11.11.11.11	175 m							
Puri Sellinge	Danan Mane	dateq								
Dury Management	Reage Profy	0								
and the second s	Report 1									
The letter	Thursd 2									
HE P Drive Accest	Incom Law B.									
The Transfer		-	100							
OFINET	10.007 20									
Andarry	Bullindo arcentado.									
ecre										
AND -										
AR	Domain Role Domain	0	Domain Name	Hasager Priority	Rang Port 1		Ring/Fort 2	Vian 3D	Rec.	mery Tane
6	E Paraja a Paraja	,,	10100	32768 #	1	_	4	1	280	*
contry	Apply Dalate									
# Appropriation										
Win port.										
gen ofer										
and the second sec										



(M)
hame

Figure 10-6 MRP Domain – Basic Settings

The following basical settings can be made:

Function	Desc
Domain Role	Clien
Domain ID's	4 UU
	00:1 [,]
	FF:F
Domain Name	Free
Ring Port 1,2	Ports
Domain VLAN ID	Sele
Recovery Time	Set t

Note

-2

- · 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.

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)

Redundancy



cription

nt or Manager depends on the inserted SD card

JID (Domain ID's) can be selected:

1:FC:FF:FF:01, 00:11:FC:FF:FF:02, 00:11:FC:FF:FF:03

F:FF:FF:FF:FF

ely selectable

s, which form the ring

ect the VLAN in which MRP operates. (1 ... 4094)

the recovery time of the ring. (200 ms or 500 ms)

• 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.

10.2.2 MRP Status

Note

1 million

												Dank Sell	ings NEP[Status
٨R	P Domain S	tatus											
	Demain Role	Domain ED	Compin None	Ring Part 1	Ring Port 1 State	Ring Port 2	Ring Post 2 State	Ring State	Ringlator	Ring Open Count	Ring Lost Open	Round Trip Dolay Min	Round Trip Delay Max
0	Cleat.	001111-1111-01	Harting	3	Stated		backed	Cient darant is care	NO FROM	2	Dires, Drain, Draws	2	3
-	Gient	00.11/c/1/002	Herting	5	boded	6	biolod	Ciant decant leave	NO EUROL	1	Uhis, Unio, 0 (403)	2	1
	Intel Intel	Inite Deslay											

MRP Domain Status window Figure 10-7

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

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

VLAN Basic Se	ettings	
Learning Mode	Maximum VL	AN ID M
IVL 💌	4094	2
мрриу		
Figure 11-1	VLAN Ba	sic Settings
This tabbed set	ection displa	ays VLAN g
Function		Descrip
Learning Mo	ode	Select the
		or SVL
		tiltering c
		this thor
		The adv
		to prever
		This mod
		a. end s
		addre
		b. learni
		In SVL, a
		Range o
		Default
Maximum V	LAN ID	Displays
Maximum Su VLANS	ipport	Displays
Number of	/LANs in	Displays
the System		switch.

	Basic Settings	Port Settings / Static VLAII / 🧿
Maximum Supported VLANs	Number	of VLANs in the System
256	1	

s tab

plobal configuration settings.

tion

e VLAN learning mode. You can enable either /VL (independent) (shared). This determines the access method to the VLAN database. In IVL, the information learnt by one VLAN is never other VLANs in making forwarding decisions. As a result of re are separate filtering databases maintained for each VLAN. antage in using IVL is that security restrictions can be applied nt unauthorized users from learning the sources of data traffic. de is typically employed in situations where...

stations operate over multiple VLANs with the same MAC ess or

ing database size is not a constraint.

a global address table is used for all VLANs combined.

of value: IVL / SVL

value: IVL

the largest valid VLAN ID that the switch allows.

the maximum number of VLANs that this switch can support.

the active number of VLANs currently configured on the

11.2 Port Settings

Basic Settings Port Settings Static VLAII (?)

HARTING

Port	PVID	Acceptable Frame Types	Ingress Filtering
E 1	1	AI I	Disabled 🖃
2	1	Al	Disabled -
C 3	1	AI	Disabled 💌
E 4	1	Al 🗾	Disabled -
5	1	Al	Disabled 🔳
6	1	Al	Disabled 💌
7	1	Al	Disabled -
	1	AL I	Disabled 💌
	1	AL	Disabled -
10	1	AI I	Disabled -

Figure 11-2 VLAN Port Settings tab

VI AN Port Setting

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

Function	Description	Function
Select/Port	This option will be checked for the port where configuration changes have been made.	VLAN ID
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	VLAN Name
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 /	Member Ports
	Default value: all frames	Untagged Ports
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	Forbidden Ports
	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	After all necessary entries a includes all existing VLANs a be changed to alter the prop or forbidden ports).

HARTING



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



		HARTING T	echnology Group
		Banic Settings / Parts	integral free states (*)
Hender Ports	Untagged Parts	Parkébéen Ports	
248	240		

escription

ere you can create a new VLAN with the specified VLAN ID. Note at an existing default VLAN which includes all ports is labelled with AN ID 1.

ange of value: 1 ... 4094

efault value: 1

becify a user-defined name, usually used to remember the purpose the VLAN.

ange of value: Not more than 20 printable characters

efault value: none

becify the ports that belong to the VLAN that you are creating.

ange of value: All

efault value: None

becify ports which forward packets untagged.

ange of value: All

efault value: None

becify ports which may not be included in the VLAN.

efault value: none

made, a list will be displayed at the bottom of the window. It ong with the user-defined information. The values in this table can ties of existing VLANs (the name, member ports, untagged 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).

12.2 802.1p Priority Mapping

	Part	Principy 0	Princip 1	Priority 2	Principy 3	Priority 4	Polocity 5	Priority 6	Priority 7	Default Printy
	1	0.00	1.14	2 14	3 10	4 m	5.00	6 M	2 14	0 M
D	2	0.000	1 M	2.8	3 (m)	1.00	5 (m)	6 M	2 M	0.001
	3	0.00	1.00	2.00	3 10	4.90	5 (w)	6 m	2 1	0 W
		0.00	1 10	2 m	3	4 m	5	6 10	7 w	0 m
	5	0.000	1.00	2 (m)	3 (m)	4 M	6 (m)	6 M	2 (m)	0.00
	6	0.000	1 14	2 [M	3 [m]	4 m	5 (m)	6.00	2 (m)	0 m
	7	0.00	1.00	2	3 (m)	4.00	5 (4)	6.00	2 1	0 (m)
		0.00	1	2.8	3 10	4.00	5.00	6.00	2 14	0 w
	9	0.00	1.14	2 14	3 10	8 m	5.00	6 M	2 14	0 M
	10	0 (m)	1.00	2(m)	3 [m]	4 (m)	8 (m)	6 M	2 (m)	* M

Quality of Service

Bank Sottings | 010.1p Priority Marping | Differs DOCP Marping | (7)

Enables or disables Quality of Service

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

Set the access order for QoS.

Range of value: First 802.1p / First DiffServ

First 802.1p

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 gueues 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

12.2.1 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

RANNE Public Publication	V. 1		100	A				1	ARTING 1	lechnology Grou
-	1							Real Senses 2 102.0	Plant, Mapping	Differential Income
mcm3402-amp	DiffServ D	SCP Table								
Evenden	9509	Priorit	,	0927	Nurity	852	Priority	8927	Printy	
in Spotence Collings		6.04	(M)	14	Arms in	10	maken an		1455-	×
T Robustery		line.	(m)	17	Aureal (at		Padan in		-44-	×.
10.48	2	1.0er	(m)	18	Aprel (m)	24	Padan M		1421	×
1H 6v5	3	Line .	(m)	19	Acres in	25	Padure (M)	91	18/1-	×
HU AP DRIVEN		Low		20	Aureal Int	26	Padun M	12	1941	×
 Rate Landing 	1	Liter	(m)	23	Assess in	27	maken int	10	140	H
H Scouly	4	Line 1	(m)		Rend in		Pater in	54	14(1)	H .
T the report	7	1.00	(m)	28	Rend in		Padan Int		Hgt-	×
1 Auro		i.m.	(m)	24	Aread in		Padun (m)	96	18/1-	×
12 Neperate		6.00	(m)	10	April 10		maken on	*	180-	×
II Statistics	10	1.04	(M)	24	Arms in	•	medium per		145-	M.
		\$ me	(m)	17	Romal an	•	Robert M.		1825	*
	12	1.00	(m)	28	Annual Inc.	**	Public M		1425	×
	10	Law	(m)	29	Aureal Inc.	•	Padun M	61	1941-	×
	14	Lin	(m)	20	Aureal in		Palue M	62	1941-	m.
	10	Liter.	(m)	21	Annual land	e	Table M	62	1451	×

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.

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.

Port	Ingress Packet Type		Ingress Limit Value	Egress Limit Value
1	broadcast	-	120K	512K 💌
2	broadcast & multicast	-	IM 💌	24
3	broadcast & multicast & flooded unit	cast 💌	401 -	84 💌
4	al	-	16M 🔟	64M 💌
5	none	-	none 💌	none 💌
6	none		none 💌	none 💌
7	none	-	none 💌	none 🖃
8	none	-	none 💌	none 💌
9	none		none 💌	none 💌
10	none	-	none 💌	none 💌

Figure 12-5

Rate Limiting

Function	Description				
Ingress Packet Type	This option defines filtering options for	s the kind of traffic which will be affected by t 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 bandwid	Ith limit for the outgoing traffic on this port.			
-	Range of value:	128 Kbit/s / 256 Kbit/s / 512 Kbit/s / 1 Mbit/s /			
		32 Mbit/s / 64 Mbit/s / 128 Mbit/s / 256 Mbit/s			

Default value:

-25

12.4 Rate Limiting

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

None

Note

the

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.

		IP Authorized Manager
IP Authorized Manag	er	
IP /	Address:	
Port List (Inc	coming):	Attention:
Services	Allowed: CALL SMMP CHTTP	The first filter configured on the switch, must have minimum one allowed service. This filter must include the workstation which should be able to gain access to the
Bold fields are required.		switch.
All		
IP Address	Port List (Incoming)	Services Allowed
Apply Delete		

IP Authorized Manager Figure 13-1

ses that you wish to allow to gain access to the n. This IP address has to be an address of an d no subnet or network address. All addresses
red to the authorization list will be blocked.
Imbers (i.e. 3-7,9) which will be controlled by the ort must be specified.
vices should be allowed or denied. If you are le, 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.

1 million

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

ATTENTION

Note

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.

802.1x Authentication:	Disabled
Authentication Mode:	Local
Network Access Server ID:	RADIUS Server
Supplicant Name:	admin
Supplicant Password:	
Supplicant Status:	unauthorized

Figure 13-2 802.1x Basic Settings tab

- ..

Function	Description
802.1xAuthentication	Specifies the s switch. Options <i>Enable</i> – enabl <i>Disable</i> – disab Range of valu Default value:
Authentication Mode	Specifies the A Range of value Default value:
Network Access Server ID	Specifies the A Packets. Range of value Default value:
Supplicant Name	Range of value:
Supplicant Password	Range of value Default value:

-				
-				
(2	20 printable character	rs)		
(2	20 printable character	rs)		
C2	20 printable character	rs)		

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

ion

_

the status of 802.1x based port security feature in the ptions are: enables 802.1x port security feature. disables 802.1x port security feature. value: Enable / Disable Disable alue: the Authentication Server Location. value: Local / Remote value: Local the Authenticator ID, which originates the Access-Request value: Not more than 20 printable characters. RADIUS Server /alue: value: Not more than 20 printable characters. admin /alue: Not more than 20 printable characters. value:

none

13.2.2 Port Settings

Basic Settings Port Settings Local Server RADRIS Settings Supplicant Session Info Timers

ielect	Port	Port Control	Auth Port Status	Auth Mode	Re-Auth	Control Direction	Operation Control Direction	Auth State	Auth Restart	Supplican Count
	1	Force Authorized	Authorized	Port Based 💌	Disable 💌	Both 🔳	Both	Force Auth	Restart	0
	2	Force Authorized	Authorized	Port Based 💌	Disable 🖃	Both 💌	Both	Force Auth	Restart	0
	3	Force Authorized	Authorized	Port Based 🖃	Disable 🖃	Both 🖃	Both	Initialse	Restart	0
	4	Force Authorized	Authorized	Port Based 💌	Disable 🖃	Both 🖃	Both	Initialise	Restart	0
	5	Force Authorized	Authorized	Port Based 💌	Disable 🖃	Both 💌	Both	Initialise	Restart	0
	6	Force Authorized	Authorized	Port Based 💌	Disable 🔳	Both 💌	Both	Initialse	Restart	0
	7	Force Authorized	Authorized	Port Based 💌	Disable 🖃	Both 💌	Both	Initialise	Restart	0
	8	Force Authorized	Authorized	Port Based 💌	Disable 🖃	Both 🖃	Both	Initialise	Restart	0
	9	Force Authorized	Authorized	Port Based 💌	Disable 🖃	Both 🖃	Both	Initialise	Restart	0
	10	Force Authorized	Authorized	Port Based	Disable -	Both .	Both	Initialise	Restart	0

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 cont	rol values of the Authenticator Port. Options are:	I	Figu
	ForceAuthorized -	 allows all the traffic through this port. 		
	ForceUnauthorize	d – blocks all the traffic through this port.	7	The
	Auto – Imposes 8	02.1x authentication process in this port.	/	Autl
	Range of value:	ForceAuthorized / ForceUnauthorized / Auto		E.
	Default value:	ForceAuthorized		Fu
Auth. Port Status	Shows the current	t status of the Authenticator Port.		Us
	Range of value:	Authorized / Unauthorized		
Auth. Mode	Specifies the conf	iguration for selecting the authentication mode.		_
	Range of value:	Port Based / MAC Based		Ра
	Default value:	Port Based		
				D -
Note				- PC

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: <i>Both / In</i> Default value: <i>Both</i>
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



HARTING

Function	Description		
Auth. Restart	Authentication Restart : to restart authentication <i>Start</i> – causes the Port <i>False</i> – reverts to False Range of value: <i>Tru</i>	specifies the initialization control of the initialization control of the initialized. The initialized of the initialization is compared of the initialization is compared of the initialization is comp The initialization is compared of the initialization of the initialization is compared of the initialization is compared of the initialization of the initialization is compared of the initialization of the	ontrol for the port
Suplicant Count	Number of supplicants	authorized on the switch	
13.2.3 Local Server			
	Basic Settings / Port Settings /	ocal Server / RADIUS Settings / Supplicant Se	ssion Info / Timers / 🕥
Local Authentication Server Conf	iguration		
User Name:	(20 printable characters)		
Password: Port List: 1-10	(as prevale or a does)		
Bold fields are required.			
A44			
User Name	Password	Port List	
Apply Delete			
Figure 13-4 Local Se	rver tab n Server Configuration p	page allows you to con	figure the Loca
Authentication Server info	ormation.		
Function	Description		
User Name	Specifies the identity of Range of value: Not Default value: nor	f the user, seeking authent more than 20 printable ch ne	cation. aracters
Password	Specifies the password Range of value: Not	l specific to the user name. t more than 20 printable ch	aracters

13.2.4 RADIUS Settings



Figure 13-5 Radius Server Configuration tab

- Default value: none
- Represents the complete set of ports of the authenticator to which the user is allowed.
- Default value: A//

Settings	Port Settings	Local Server	RADRIS Settings	Supplicant Session In	fo / Timers / 🕐
et	Server Typ	e R	esponse Time (sec)	Retr	r Count

HARTIN

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

Function	Description	
IP Address	Specifies the IP Ad	dress of the RADIUS Server.
Shared Secret	Specifies the secr RADIUS Server an Range of value: Default value:	et string, which is to be shared between the d the RADIUS Client. Not more than 20 printable characters. none
Server Type	Specifies the RAD Range of value: Default value:	US server type <i>Authenticating / Accounting / Both</i> <i>Both</i>
Response Time	Specifies the maxir respond to a reque Range of value: Default value:	num time within which the Radius Server has to est from the Radius Client. <i>1 120 sec</i> <i>20 sec</i>
Retry Count	Specifies the maxin re-transmitted befor Range of value: Default value:	mum number of times a radius request is to be re getting response from the Radius Server. 1 254 100

13.2.5 Supplicant Session Info

 Basic Settings
 Port Settings
 Local Server
 RADUS Settings
 Supplicant Session Info
 Timers
 Timers</t

Figure 13-6 Supplicant Session Info tab

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

13.2.6 Timers

mer	8									
elect	Port	Quiet Period (sec)	Transmit Period (sec)	Re-Auth Period (sec)	Supplicant Timeout (sec)	Server Timeout (sec)	Held Period (sec)	Auth Period (sec)	Start Period (sec)	Auth Retries
	1	60	30	3600	30	30	60	30	30	2
	2	60	30	3600	30	30	60	30	30	2
	3	60	30	3600	30	30	60	30	30	2
	4	60	30	3600	30	30	60	30	30	2
	5	60	30	3600	30	30	60	30	30	2
	6	60	30	3600	30	30	60	30	30	2
	7	60	30	3600	30	30	60	30	30	2
	8	60	30	3600	30	30	60	30	30	2
	9	60	30	3600	30	30	60	30	30	2
	10	60	30	3600	30	30	60	30	30	2

Figure 13-7 Timers tab

Function

Quiet Period

Transmit Period

Re-Auth. Period

Held Period

Auth Period

The 802.1x Timer Configuration individual port level.

	Desc
	Speci
	will no
	Rang
	Defau
	Speci
	the E/
	Rang
	Defau
	Speci
	suppli
	Rang
	Defau
ut	Speci
	transr
	authe
	Rang
	Delat
	0
	Speci
	Speci transr
	Speci transr relaye
	Speci transr relaye Rang Defau
	Speci transr relaye Rang Defau Speci
	Speci transr relaye Rang Defau Speci a faile
	Speci transr relaye Rang Defau Speci a faile Rang
	Speci transr relaye Rang Defau Speci a faile Rang Defau
	Speci transr relaye Rang Defau Speci a faile Rang Defau Speci
	Speci transr relaye Rang Defau Speci a faile Rang Defau Speci after r
	Speci transr relaye Rang Defau Speci a faile Rang Defau Speci after r Rang
	Speci transr relaye Rang Defau Speci a faile Rang Defau Speci after r Rang Defau
	Speci transr relaye Rang Defau Speci a faile Rang Defau Speci after r Rang Defau

Security

The 802.1x Timer Configuration page allows you to configure the Timer parameters at the

ription

ifies the duration for which the authenticator remains silent and ot attempt to acquire a supplicant.

- **ge of value:** 0 ... 65 535 sec
- ult value: 60 sec

ifies the time period used by the authenticator to define when APOL PDU has to be transmitted.

- ge of value: 1 ... 65 535 sec
- ult value: 30 sec

ifies the time between periodic re-authentication of the licant.

- ge of value: 1 ... 65 535 sec
- ult value: 3600 sec

ifies how long the switch waits for a response before remitting the request to the client if a request is relayed from the entication-server to the client.

- ge of value: 1 ... 65 535 sec
- ult value: 30 sec
- ifies how long the switch waits for a response before remitting the request to the authentication server if a request is ed from the client to the server.
- **ge of value:** 1 ... 65 535 sec
- ult value: 30 sec
- ifies the amount of time the client will wait before re-attempting ed 802.1X authentication.
- ge of value: 1 ... 65 535 sec
- ult value: 60 sec
- ifies the time interval for resending 802.1X request messages not receiving a response.
- **ge of value:** 1 ... 65 535 sec
- ult 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.

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

Link Aggregation Basic Set	tings		
UA Status	Deathd M		
Sutan Harts: Sutan Id	40 40 40 40 00 00 00		
- Ap. Ac			
Figure 14-1	Link Aggre	gation Basic Setting	s tab
-		-	
Function		Description	
Link Aggrega	ation	The Link Aggrega	tion module administrative status. Options are:
Status Speci	fies	Enabled	Enables Link Aggregation in the switch.
		Disabled	Disables Link Aggregation in the switch.
		Range of value:	Enable / Disable
		Default value:	Disable
System Prior	itv	Defines the system	m priority
Oystelli i Hoi	ity	Banga of value:	0 65 525
		Range of value.	0000000
		Default value:	32 768
System Id		Shows the system	n ID (MAC Address).
-			

· All member links are interconnected between two identical end nodes.



ARTING

14.3 Port Settings

HARTIN

14.2 Interface Settings

					and the second s	and the president	
Link Aggregation Interface S	Settingo						
Part Charmel 88							
Admin Status:	form M						
Beld folds are required.							
A46							
East Charged M	Admin Male	Energy insulations of states	Marcha .	Barts	to of Eastering Channel	4	
Fund Constraints	Noner Flage	Cycle and a state		Peru		-	

Figure 14-2 Link Aggregation Interface Settings tab

			Control
Function	Description	App	
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	Figure 14-3 Link A	Aggregation Pol
	normal port inside the switch.	Function	Descrip
dmin Statua	Administrative control of a Dart Channel: aposition the Admin status	Port	Specifie
annin Status	of the port channel	Port Priority	Specifie
	Range of value: Un / Down		If the n
	Default value: Down		supporte
)per State	Specifies the operational status of the port channel. This is a read-		active lir
	only field.		Range o
S	All port channels are shown in the table. Each channel can be	Mode	Link Age
- B	shutdown or deleted individually by the administrator.		and LAC
lode	Link Aggregation can be configured in two different ways: Manual		work as
	and LACP.		configura
	The Manual configuration will set the specific ports immediately to		To minir
	work as a trunk port. If the ports on the neighbour switch are not		of manu
	configurate as manual ports, the connections may cause loops.		without u
	To minimize the appearance of failures during the configuration		The dyn
	of manual Link Aggregation, the switches should be configurated		to a neg
	The dynamic configuration with the LACP will set the specific parts		the neig
	to a negotiation state before acting as a trunk port. If the ports on		or failure
	the neighbour switch are not configurated as LACP ports, no loops	Activity	Specifies
	or failures will occur.		Active:
	Range of value: Manual / LACP / Disable		Passive:
	Default value: Disable		Pango (
Ports	Specifies the interface indices that must be configured to be		Default
	members of the Port Channel.	Timeout	Specifie
No of Ports Per	Indicates the number of ports that are bundled per port channel.	Timoout	port to a
Channel			Long:
			0 / ⁻ /

Link Aggregation

Busic Settings / Interface Settings / Part Settings (3)

Timeout		Wall Time (sec)	Dande State
LING	(m)	2	Dente
Long		2	Dawn
Long	m	2	Deven
Long	(m)	1	Daven
Long		2	Down
Long	-	2	Deven
Long	(m)	2	Daven
Love	x	2	Deve
Long	(m)	2	Deven
Long	(m)	2	Deven

ion Port Settings tab

escription

pecifies the Interface Index.

pecifies the Priority value of the port.

the number of links in an aggregation exceeds the maximum upported by the hardware, the links with lower priority become ctive links.

ange of value: 0 ... 65535

nk Aggregation can be configured in two different ways: Manual nd LACP.

ne Manual configuration will set the specific ports immediately to ork as a trunk port. If the ports on the neighbour switch are not onfigurate as manual ports, the connections may cause loops. minimize the appearance of failures during the configuration manual Link Aggregation, the switches should be configurated thout using redundant connections.

ne dynamic configuration with the LACP will set the specific ports a negotiation state before acting as a trunk port. If the ports on e neighbour switch are not configurated as LACP ports, no loops failures will occure.

becifies the Port LACP Activity. Options are: Active and Passive.

LACP negotiation is started un-conditionally

LACP negotiation is started only when LACP packet is received from peer

ange of value: Active / Passive

efault value: Active

pecifies the time within which LACP PDUs must be received on a ort to avoid timing out of the Aggregated Link. Options are:

ong: 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

Description

immediately.

Options are:

Standby:

Down:

Default value:

and before entering aggregation.

Range of value: 0 ... 10 sec

2 sec

Specifies the waiting time for a port after receiving Partner information

Configuring the wait-time value as 0 ensures that links get aggregated

Indicates the current state of the port with respect to Link Aggregation.

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

The port is a member of the port channel but is

its Oper-Status is Up.

currently in standby state.

The Ports Oper-Status is Down.

Function

Wait Time(secs)

Bundle State



15.	Mult	icast
-----	------	-------

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.



GMRP and IGMP Snooping cannot operate at the same time!

The following tabbed sections are available:

15.2 Basic Settings

GMP Snooping Basic Set	tings	
10HP Scorping Rulas	Operational Status	
Deated an	Desided	

Figure 15-1 IGMP Snooping Basic Settings tab

Function	Description	
IGMP Snooping Status	Select <i>Enable</i> to e switch. If this set possible.	enable IGMP snooping globally throughout this ting is disabled, no interface configuration is
	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 router ports only.	IGMP reports to be forwarded on all ports or on
	Range of value: Default value:	All ports / Router ports / None-Edge ports All ports



I



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 portsDefault value:All ports
Query Transmit on TC	Select <i>Enabled</i> or <i>Disabled</i> to specify whether IGMP snooping queries are transmitted after a topology change. <i>Enabled</i> activates query transmissions. Range of value: <i>Enable Disable</i> Default value: <i>Enable</i>
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

				DRINK S-OTSINGS	Tanger	store certagos store.	Roster Ports	search and Group
IGMP Snooping Timer Configurati	om							
Router Port Parge Entered On Cit	125							
Group Phenton Port Purge Ethernal (sec)	250							
Report Parward Different (sec)	5							
Grap Quey Hervel (sec)	2							
bald fields are required.								
Amh								

IGMP Timer tab Figure 15-2

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

ARTING



Figure 15-3

Function

VLAN ID

IGMP Snooping Status

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:

Multicast

			Basic Settings	Bear, / 1	ALC: Configuration	Roster Ports	Multicest George
gured Quesier	Current Querier Status	Querier Internal (sec)	Rauter Part List	Startup Quer Count	y Statup Query (sec)	Internal Other	Queries Present val (ser)

IGMP Snooping VLAN Configuration tab

Description

```
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
Select to enable or disable snooping on the specific VLAN. You can
        snooping for a specific VLAN even if snooping in enabled
       y in the Basic Settings tab.
       of value: Enable / Disable
       It value:
                  Enable
       the IGMP version which should be used on this switch.
       of value: Version 1 / Version 2 / Version 3
       It value:
                  Version 3
       whether the fast leave processing should be enabled or
       d on the specified VLAN.
       of value: Enable / Disable
                  Enable
       t value:
       whether the IGMP snooping switch should be enabled or
       ed as a querier on a specific VLAN.
       of value: Enable / Disable
       It value:
                  Enable
        the interval (in seconds) used to send general queries by the
       when it is configured as a querier.
       of value: 60 ... 600 sec
       t value: 125 sec
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).



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 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	Descript
Link Up / Link Down	Specify, up or do boxes.
System Events	Check a <i>address</i> trigger a
Receiver	Specify SMTP se tab in ore

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: \leq (<i>Query Interval/4</i>) 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

		Back Softenge	Ince	WLASS Configuration	Rodar Ports	Multicost Group	6.0
IGMP Snooping VLAN Router Ports							
R.41 20 Per	et that						
1							

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

		Dank Settings	Timer	VLAB Configuration	Touter Parts	Multicard Group	0
IGMP Snooping Multica	st Group						
WAN ID	Groups MAC Address			Port List			
1	OLDERSON/PUT PA			3			

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.

This section allows you to create two distinct e-mail alert profiles; these profiles are maintained

ption

t, on a per-port basis, if an e-mail is sent when a link is brought lown by checking one or both of the *Link Up* and *Link Down*

a box next to the appropriate event: *Save Config*, *New IP* s and *Power Failure*. If a checked event takes place, it will an *E-Mail Alert*.

the *To:*, *CC:* and *Subject:* fields for the alert e-mail. The server information must also be correctly specified in the next order to send e-mail from the switch.

16.1.2 SMTP Server

	Alarm 1	Alarm 2	SMTP Server	۲
SMTP Settings				
SMIP - Server:				
Bold fields are required.				
Apply				

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.

		/ he ///2
SNMP Trap		
Trap Rasaiwar		
Advata Nap Ir		
Raceiver & IP-Address		
Activita Ikap 21		
Raceiver-21P-Address		
Port Events		
Port	On Link Change	
1	0	
•		
•		
•	0	
0 *	0	
□ +		
	0	
•	0	
D •		

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 <i>Active</i> 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

								Ingress	State E	gress Sta	ts / Hist	ogram
ngre	ess Statistic	:5										
Port	Good Octets	Bad Octets	Unicast Pkts	Multicast Pkts	Broadcast Pkts	Pause Frames	Undersize	Fragments	Oversize	Jabber	Rx Error	FCS Erro
1	13103179	0	148650	36	5245	0	0	0	0	0	0	0
2	0200941	0	06506	13	237	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0



Figure 17-1

Ingress Statistics tab

Function	Descri
Clear counter	This op
Bad Octets	Amoun
Unicast Pkts	The tot
	unicast

ption

otion will clear all ingress counter of the switch.

nt of bad octets received on that port

tal 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

Ingress Stats / Egress Stats / Histogram / 🥎 Egress Statistics Port Out Octets Unicasts Pkts Multicast Pkts Broadcast Pkts Pause Frames Deferred Collisi Single 1 18292386 89277 132558 226 10 0 0 0 13006420 3739 0 7 0 0 0 0 0 0 0 0 9 0 0 0 0 0 0 0 10 0 0 0 **Clear Counter**





Function

Out Octets

Deferred

Collisions

Single

Multiple

Excessive

FCS Error

Late

- This option will clear all egress counter of the switch.
- The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS
- The total number of good packets sent that were directed to a unicast address.
- The total number of good packets sent that were directed to a multicast address.
- The total number of good packets sent that were directed to the broadcast address.
- The total number of flow control messages that were sent.
- 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).
- The best estimate of the total number of collisions on this Ethernet segment. This counter is applicable in half-duplex only.
- The total number of successfully transmitted frames that experienced one collision. This counter is applicable in half-duplex only.
- The total number of successfully transmitted frames that experienced more than one collision. This counter is applicable in half-duplex
- The total number of frames that were dropped because the frame experienced 16 consecutive collisions. This counter is applicable in half-duplex only.
- The total number of late collisions (detection later than 512 bit-times into the transmission of a frame). This counter is applicable in half-
- The total number of frames transmitted with an invalid FCS.

17.1.3 Histogram

	Hs	togram Mode: Both	-			
A	ply .		_			
ort	64 Octets	65-127 Octets	128-255 Octets	256-511 Octets	512-1023 Octets	1024-Max Octets
	140117	222167	11770	532	508	1035
	10550	221492	11620	337	7	25
	0	0	0	0	0	0
	0	0	0	0	0	0
	0	0	0	0	0	0
	0	0	0	0	0	0
	0	0	0	0	0	0
	0	0	0	0	0	0
	0	0	0	0	0	0
0	0	0	0	0	0	0
Clear	Counter					



Figure 17-3 Histogram tab

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



ARTING

HARTING

17.2 Port Mirroring

C3

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.

	Part Mirroring Status:	Onebled	(m)		
	Plonito Fisit				
Port Opt	liona				
P.	et			HenringD	, diam
0 2					
0 2					
• □					
5					
6					
01					
• □					
•					
D 22				Deabled	

Figure 17-4

FunctionDesPort Mirroring StatusSele

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 checkb
Monitor Port	Select (monito
Mirroring Option	the min Select i or if you



Port Mirroring section

Description

Select Enabled or Disabled to enable or disable port mirroring globally.

the port that you would like to change by clicking on the pox here.

the port that you would like to use as your diagnostic or) port. Only one port can be selected. This port will receive rored traffic.

if you want to mirror the incoming traffic or the outgoing traffic ou want to mirror both.

HARTIN

17.3 Switch History **Event Message** Switch History deleted This section lists a system log of all significant switch events. The one-hundred most-recent SYSTEM IS STARTING ... events are listed in chronological order. This list is maintained until the switch is rebooted or until The switch has detected low su the user deletes the list using the Clear button. power Switch History 🤊 Configuration was saved Switch History IP address has been changed Event No. Event Date SysUpTime Web login successful Web login successful 22:17:15 01.01.00 22 hours, 17 minutes and 25 seconds. Web login successful 00:04:56 01.01.00 5 minutes and 7 seconds. Web login expired 8 Link status up on interface Fa0/6 00:00:04 01.01.00 15 seconds Link status up on interface Fa0/1 00:00:04 01.01.00 15 seconds. Ip address has been changed Web login failure 00:00:03 01.01.00 14 seconds 00:00:03 01.01.00 14 seconds. Ip address has been changed Link status down on interface Fa0)6 00:00:03 01.01.00 14 seconds. User admin logged in via telnet 00:00:02 01.01.00 14 seconds. Link status down on interface Fa0/1 Firmware: 2.1.1.1 (hv=M8-2 V1.0, d-tm=Nov 25 2009-10:36:48) <IP-Address> 00:00:10 01.01.00 0 seconds. SYSTEM IS STARTING 01.01.00 User admin logged out via telnet Clear Refresh <IP-Address> Attempt to login as admin via te Figure 17-5 Switch History event list from <IP-Address> failed User admin logged in via ssh from Function Description Address> Event No. Switch events are numbered in decreasing order as they occur. User admin logged out via ssh Max. 100 events are reported. <IP-Address> Attempt to login as admin via te Note from <IP-Address> failed The counter starts with 1. New events will be inserted on the first line of the list, so that the oldest Firmware update was initiated event (with the lowest number) will move downwards. If more than 100 events reported, the Firmware update failed oldest events will be deleted on the bottom line of this list. Firmware Update aborted Event No. Switch events are numbered in decreasing order as they occur. Link status <up|down> on interface Max. 100 events are reported. 0/<port-number> Displays a text message which describes the event which occurred. Event Admin status <up|down> on inter Fa 0/<port-number> Time / Date Displays the time and date that the event occurred in the format hours:minutes:seconds and day.month.year. Got time from <SNTP-serve address>(a.<SNTP-server-index) SysUp Time Displays the time elapsed from when the system was last powered on to when the event occurred. Writing new <config-file> with def values 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 Set to factory default operation fail the view. Send email message: <message-t Refresh Click on this button to update the list with the most current events. Send email failure: <error-messag Event messages are explained in the table an p.77. hTrap: <error-message>

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></ip-address>	Log in to the command line interface via telnet was successful
User admin logged out via telnet from <ip-address></ip-address>	Log out from the command line interface via telnet was successful
Attempt to login as admin via telnet from <ip-address> failed</ip-address>	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></ip- 	Log in to the command line interface via ssh was successful
User admin logged out via ssh from <ip-address></ip-address>	Log out from the command line interface via ssh was successful
Attempt to login as admin via telnet from <ip-address> failed</ip-address>	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></port-number></up down>	Indicates that a device was connected/ disconnected at the specific interface
Admin status <up down> on interface Fa 0/<port-number></port-number></up down>	Indicates that the user has enabled/disabled the specific interface
Got time from <sntp-server-ip- address>(a <sntp-server-index)< td=""><td>Date and Time synchronised synchronized successfully with one of the configured server</td></sntp-server-index)<></sntp-server-ip- 	Date and Time synchronised synchronized successfully with one of the configured server
Writing new <config-file> with default values</config-file>	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></message-text>	An email was successfully relayed to the SMTP- server
Send email failure: <error-message></error-message>	Sending the email failed
hTrap: <error-message></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=""></ring></domain 	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

Al Parts (m)				
Index	1442	Teler	Port	VERN
	00.00xC0-0C6DCF	Learned	3	
:	00.00.0C/CE109.44	Learned	5	1
5	00.0030005119.50	Leaned	1	1
(00 11/FC/00 8CHC0	Learned	3	1
1	00.10/PCOV 69.69	teaned	9	1
	30 11/PC/35 12:40	Learned	3	
7	00.11/FO/8-32/80	Laared	3	1
	\$0.11/PC/36.04.00	teaned	9	1
	80-11-PC-05-C7-20	Learned	3	
10	20.11/F0.05-CF #0	Leared	3	1
21	00111/PC06/1C/00	Learned	9	1
12	10 11 / C 04 94 CT	Learned		1
13	00.11/FC08-30.60	Leared	,	1
	80111/PC09-481/02	Learned	3	1
15	2011/7036-6540	Learned	3	
26	00.11/FC06.48/29	Leared	3	1
17	0011R06/725R34	Learned	3	1
18	00.23/54 IC 07/15	teaned	3	
79	00 A0/503-470F	Learned	1	1
20	00 40 42 22 49 497	Learned	3	1

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 <i>All Ports</i> and click on the <i>Apply</i> 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.
Туре	Displays whether the MAC address was learned automatically by the switch or if it was entered manually. <i>Unlearned</i> 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 <i>All Ports</i> 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.

ARTIN

HARTIN

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.

Light Beacon	
Light Beacon	
(1 - 10 sec)	
Bat	
iaure 17-7	Light Beacon funct

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.

Sent Pits: 3	Average Time (ms): 40
Ping fu	inctionality
	Descrip
	The IP-
	Dango
	Sert Pits: 3 Ping fu

LightBearen (2)

Light Beacon functionality

Ping 🧿 Min Time (ms): 30

ption

Address of the destination of value: IP-Address inside the switch subnet value: none

Function	Descri
Transmitted Unicast Packets	Display destina
Transmitted	Display
NonUnicast Packets	type br
Transmitted Discards	Display or path
Transmitted Errors	Display

18.1.2 Ethernet Statistics

Index	Alignment Errors	FCS Errors	Single Collision Frames	Multiple Collision Frames	SQE Test Errors	Deferred Transmissions	Late Collisions	Excess Collisions	Transmitted Internal MAC Errors	Carrier Sense Errors	Frame Too Long	Received Internal MAC Errors	Symbol Errors	Duples Status
1	0	0	0	0	0	0	0	0	0	0	0	0	0	ful duplex
2	0	0	0	0	0	0	0	0	0	0	0	0	0	half duplex
3	0	0	0	0	0	0	0	0	0	0	0	0	0	half
4	0	0	0	0	0	0	0	0	0	0	0	0	0	half
s	0	0	0	0	0	0	0	0	0	0	0	0	0	half
6	0	0	0	0	0	0	0	0	0	0	0	0	0	half
7	0	0	0	0	0	0	0	0	0	0	0	0	0	full duplex
8	0	0	0	0	0	0	0	0	0	0	0	0	0	half
9	0	0	0	0	0	0	0	0	0	0	0	0	0	half
10	0	0	0	0	0	0	0	0	0	0	0	0	0	half

Figure 18-2 Ethernet Statistics tab

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

ice information on utilization and errors. The					
	Function	Description			
	Port	Display the Port number on th			
ber on the switch.	Alignment Errors	Displays the number of alignment			
tes of the MTU (Maximum Transmission Unit)	FCS Errors	Displays the number of erro Sequence octets.			
the port in bits per second. This is dependent	Single Collision Frames	Displays the count of succ interface for which transmission			
of bytes (octets) received on the port since last	Multiple Collision Frames	Displays the count of successful for which transmission is delay			
umber of packets received with a specific	SQE Test Errors	Displays the number of times for this port.			
nber of non-unicast packets received with no f type broadcast or multicast).	Deferred Transmissions	Displays the number of frame delayed because the medium			
of packets received and discarded. This can	Late Collisions	Displays the number of times 512 bit-times after the packet?			
of incoming packets discarded due to format sized oversized or improper-FCS packets)	Excess Collisions	Displays the number of frames due to too many collisions.			
of IP data packets received and discarded	Transmitted Internal MAC Errors	Displays the number of fran because of an internal MAC s			
umber of transmitted bytes (including bad on that port.	Carrier Sense Errors	Displays the number of times when attempting a frame trans			

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

Interface Ethernet 🤄

HARTIN

Port	мти	Speed (Mbits/sec)	Received Octets	Received Unicast Packets	Received NonUnicast Packets	Received Discards	Received Errors	Received Unknown Protocols	Transmitted Octets	Transmitted Unicast Packets	Transmitted NonUnicast Packets	Transmitted Discards	Transmitte Errors
1	1500	100	1206209	7093	0	0	0	0	7502909	9167	0	0	0
2	1500	10	0	0	0	0	0	0	0	0	0	0	0
3	1500	10	0	0	0	0	0	0	0	0	0	0	0
4	1500	10	0	0	0	0	0	0	0	0	0	0	0
5	1500	10	0	0	0	0	0	0	0	0	0	0	0
6	1500	10	0	0	0	0	0	0	0	0	0	0	0
7	1500	10	0	0	0	0	0	0	0	0	0	0	0
8	1500	10	0	0	0	0	0	0	0	0	0	0	0
9	1500	10	0	0	0	0	0	0	0	0	0	0	0
10	1500	10	0	0	0	0	0	0	0	0	0	0	0

Figure 18-1 Interface Statistics tab

The Interface Statistics tab displays per-port devi 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 <i>broadcast</i> or <i>multicast</i>).
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	Displays the number of IP data packets received and discarded
Protocols	because of an unsupported or unknown protocol.
Transmitted Octets	Displays the total number of transmitted bytes (including bad packets) transmitted on that port.

Interface Ethernet

ption

ys the total number of packets transmitted with a specific ation (unicast).

ys the total number of non-unicast packets transmitted (of roadcast or multicast).

ys the number of packets dropped due to network congestion error.

ys the number of packets discarded due to format errors.

ne switch

ment errors received.

ors involving incoming Frame Check

ccessfully-transmitted frames on the ion is delayed by one collision.

fully-transmitted frames on the interface ayed by more than one collision.

that the SQE test error was generated

nes where the initial transmission was was busy.

that a collision was detected at a point 's transmission.

es on the interface for frames that failed

me errors where transmission failed sub-layer error.

s the carrier sense condition was lost nsmission on the port.



HARTIN

18.3 IGMP Snooping Statistics

ARTIN

18.3.1 IGS Statistics

the statistics in these columns.

GS S	statistics									
VLAN ID	General Queries Received	Group Queries Received	Group & Source Queries Received	IGMP Reports Received	IGMP Leaves Received	IGMP Packets Dropped	General Queries Transmitted	Group Queries Transmitted	IGMP Reports Transmitted	IGMP Leaves Transmitted
1	0	0	0	0	0	0	495	0	0	0

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.

IGS V3 Statistics									
VLAN ID	V3 Reports Received	IS_INCL Messages Received	15_EXCL Messages Received	TO_INCL Messages Received	TO_EXCL Messages Received	ALLOW Messages Received	BLOCK Messages Received	V3 Reports Sent	
1	497	0	0	0	0	0	0	0	

Figure 18-6 IGS V3 Statistics tab

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	Displays the number of frame errors where reception failed because
MAC Errors	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

								formation	Port Statistics
RSTP Information									
Protocol Specification	Time Nece Topelogy Change	Designated Rect	Root Cost	Root Part	Max Age (sec)	Hello Time (sec)	Hold Time	Forward	Delay (sec)
ieee0021d	0 hrs, 13 mm, 50 secs	80.00.00.01.70.00.40.09	40000	3	20	2		25	

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.

										Informat	tion Pe	art Statistics	0
RST	P Port S	tatistics											
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

Statistics

IGS Statistics | IGS V3 Statistics | ?

This tab displays general IGMP statistics. Refer to RFC 2236 for detailed information concerning

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:



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

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).

-3

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.
- special file name.
- SD card
- the internal flash.

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.

SD Memory Card (optional)

At a time, only one configuration can be stored on the memory card. This configuration has a

 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

· When an SD card is plugged in, the switch stores the configuration always on the SD card and

· To save a configuration on the SD card it has to be unlocked.

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.

Dig Station Edit Insert PLC View	Options Window Help		
🗅 🚅 🔓 🔍 🖏 📇 📾 🖻	Customize	Ctrl+Alt+E	
≥(U) UR	Specify Module Configure Network Symbol Table Report System Error	Ctrl+Alt+T	
2 CPU 315-2 PN X1 MPL/DP X2 PN-IO	Edit Catalog Profile Update Catalog		Ethemet(1). PROFIN
X2PIR Port 1	Install HW Updates		
3	Install GSD File		
J _A	Find in Service & Support		
	Create GSD file for I-Device	here .	

Figure 20-1 Installing the GSD file



Figure 20-2 Select GSD file



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.

-25

HARTIN

Configuration with Automation Software Tool

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

	×
•	
2AASFP-SWITCH-20130712.1	Browse
Release 2.xml 07/12/2013 12:00:00 A	Version Lang M V2.3 Engli
Deselect All	
	Help

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

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.

perces - inconditi	2-0031	
eneral		
Shot description:	mCon3102-AASFP	
	HARTING Managed Switch with 10 Elnemet Parts; PROFINET ID device; PROFINET interface	*
Order No./ firmware:	20751124300 / V3.5	
Family:	HARTING He-VIS Switch	
Device name:	edak/1021/A/STP	_
· Node in PROFINET	Orange Release Number	
Device number:	PROFINET-IO-System (130)	
IP address:	192.168.0.3 Elvernet	
P Assign IP addres	s via IO controller	
Comment:		
		*

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



Figure 20-7

20.2 Hardware Configuration

liot	Module	Order number	I address	Q address	Diagnostic address:	Comment
0	BCon3102 AASFP	20761124300			2032"	
87	PN-10				2007*	
KT P1b	Flat Ib				2020	
17 F20	Port 2b				2029*	
X1 F3	Aut 3				2028*	
17 FV	Pat 4				2027~	
775	Part 5				2235"	
(7 FB	Part 6				2025*	
(1 F?	Aut 7				2024*	
CT P8	Part 8				2023*	
17.79	Part 9				2022~	
KT F10	Part 10				2021*	
	QoS configuration				2020*	
	Global I/O		0	0		
1	Port L/D		12	12		

Figure 20-8

HARTIN

Configuration with Automation Software Tool

9. Select the relevant device and assign the name.

pe: HARTING Ha-VI	S Switch
	Assign name
witch	
witch	Node flashing test Duration (seconds): 3 Flashing on Flashing off
vices without names	
	Help

Select the switch and assign the names

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

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

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

erties - mCon3102-AASFP (R-/50 General Addresses Parameters - Recompleters
 Parameters

 Brake Dagnosis

 - B Missio Card In Sect

 - B Missio Card In Sect

 - B Low Yoltage detected (US1 or US2)

 Don't send dagnosi

 - B Low Yoltage detected (US1 or US2)

 - D hitsend dagnosi
 ОК Cancel Help

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



Figure 20-11

Function	Values
Tranmission medium / duplex	Disable
	Automa
	Automa
	TP/FO 1
	TP/FO 1

HARTING

Configuration with Automation Software Tool

	×
ather pot.	
2	
Detals	
grad delay time: 0.60 ps)	
Cancel Help	

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

Transmission medium / duplex settings

natic Settings

natic Settings (monitor)

100 Mbps full duplex (Depending on the device used)

1000 Mbps full duplex (Depending on the device used)



HARTIN

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.

🛛 😋 Parameters	Value	
Carl Disposis	Don't send diagnosis	

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.

C Departmenter	Value	
Configuration of QoS parameters	A description of the later	
Queung Scheme	Automatic/System-Default	

Figure 20-13 QoS settings

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

Function	Values
Queuing Scheme	Autom
	8-4-2-2
	Strict E

20.2.5 Slot 2: Global IO Data

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

Bit	Value	Meaning
0	0	-
1	0	-
2	0	-
3	0	-
4	0	-
5	0	-
6	0	-
7	0	-

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	

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

Configuration with Automation Software Tool

natic/System-Defaults 1 weighted Strict Priority Queuing

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

By	y	te	2	

value	Meaning
1	Port 9 is UP
1	Port 10 is UP
1	-
1	-
1	-
1	-
1	-
1	-

Configuration with Automation Software Tool

Appendix Glossary of	f Terms and Abbre	eviations	Half Duplex	A netw both di
	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.	HTTP (HyperText Transport Protocol)	before A com
	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		used b Ethern
	Boot	The process of starting up a device and loading the operating system.	for Electrical and Electronics Engineers)	for sett
	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.	IGMP (Internet Group Management Protocol)	A prote groups them t
	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.	IGMP Snooping	A meth so that bandw
	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.	Import	The pro file fror
	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	IP (Internet Protocol)	The brock protoco formate
		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 <i>Dynamic</i> .	IP Address	Anume The Et at the f user L/
	Ethernet	An IEEE standard networking protocol. The protocol describes a frame-based technology for sending out and receiving from a	LAN (Local Area Network)	The gr networ mask.
	Export	The process of transferring (uploading) a saved configuration or firmware file from the Ethernet switch to a TETP server	Link Aggregation	A trunk group o
	Fast Ethernet	An Ethernet network capable of operating at 100 Mbit/s.	MAC (Media Access Control) Address	The u
	Firmware	The programming code used by the switch for its basic operating functions. The Ethernet switch firmware operating system can be		connect two Eth
	Flow Control	upgraded by overwriting it with a new firmware version. 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	Managed Switch	An intended of the as a weight of the second
		overrun with data.	MIB (Management	A data
	Full Duplex	The ability of a network connection to handle communication in both directions simultaneously.	Information Base) Mirroring	a netwo A proc
	Gigabit Ethernet	An Ethernet network capable of operating at 1000 Mbit/s (1 Gbit/s).		and se

work connection that is not capable of communications in irections simultaneously. Communication in both directions is le, but each device must wait for the other to stop transmitting replying.

munication protocol used between a web browser and web . HTTP is used throughout the world wide web and is also between the client web browser and the web server on the net switch.

erican organization created in 1963 that has been responsible ting standards for communications.

tocol used to manage the membership within IP multicast s. It enables hosts to notify a local router or switch and inform that they would like to receive transmissions assigned to a ic multicast group.

hod where a switch listens ("snoops") in on IGMP messages t it can optimize the traffic flow. IGMP snooping is able to limit vidth-intensive traffic (such as streaming video) to only the ic requestors. Flooding of the entire network is then avoided.

rocess of transferring (downloading) a configuration or firmware m a TFTP server to the Ethernet switch.

road-based protocol used in the Internet layer of the Internet col suite. The IP protocol defines addressing and data packet ts.

eric address used to identify a computer or device on a network. thernet switch has a default IP address of *192.168.0.126* set factory. A new, unique IP address should be assigned to fit the AN.

group of computers and devices that populate your local rk. The address range of a LAN can be defined by the subnet

king strategy which optimizes available resources by linking a of ports together to form a single trunk.

unique, physical address assigned to a device by the acturer. The switch maintains a MAC address table of cted devices. These addresses are used for sending layer-hernet frames to a specific host.

telligent device which filters and forwards packets between rk segments. A managed switch features one or more ways a user to directly access and configure switch operations (such web or command-line interface).

abase used by SNMP to describe and manage devices within vork.

ess where data flow from or to a particular port is duplicated ant to another port for monitoring purposes.

HARTIN

Configuration with Automation Software Tool

Multicast	A method of network addressing used to deliver information to a group of targets simultaneously. Multicast addressing attempts to	SNMP V1	An earlier communit
	implement the most efficient strategy possible for delivery and creates copies of data streams only when links to multiple destinations split apart.	SNMP V3	The current control an
Packet	A discrete unit of data sent out over a network.	Subnet	A group of prefix. All
Port	A connection jack on a switch or device which is used for plugging in connections to other devices.	Output	hop witho
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.	Subnet mask Switch	address. T prefix as u 255.255.2 IP address A device
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.	TFTP (Trivial File Transfer Protocol)	LAN. A s sophistica A simplifie switch to firmware
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.	VLAN (Virtual Local Area Network)	by the TF A logical s attached t
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.		

- lier version of SNMP where security is based only on private unity strings.
- rrent version of SNMP with support for authentication, access and privacy.
- o of networked computers that all share a common IP address All devices within the same IP subnet can be reached in one hout a router.
- P decimal representation for the subnet prefix of the IP s. The subnet mask specifies the length of the shared subnet as used by all devices in the local subnet. A subnet mask of *5.255.255* is used by the Ethernet switch to isolate a specific ress.
- ce that connects several LANs together to form one logical A switch is similar to a bridge, but usually offers more cicated features for bridging LANs of different types.
- lified version of the TCP/IP file transfer protocol used by the to transfer saved configuration profiles and to perform new re updates. The switch can download new firmware from a ter's TFTP server. A username and password are not required TFTP protocol.
- al subgroup which acts like a LAN and communicates as if ed to one broadcast domain.

Т

Index

Α	
Admin password	24
Alarm profiles	69
Alert	69
Alignment errors	81
Auto-negotiation 18, 22,	94
В	
BPDU	41
С	
Carrier Sense	81
Class Field	50
Collision	94
Collision frames	81
Counters	80
D	
– Data packets	80
Designated bridge	43
Designated root	43
DHCP	94
DHCP Option 82	33
DiffServ	52
Discards	80
DSCP	50
Duplex	22
Duplex mode	18
E	
– Edge port	43
E-mail alert	69
_	
	~ (
	34
Firmware version	17
	22
	94
G	
н	
Hardware version	17
Ha-VIS mCon Ethernet Switch	7

IEEE 802.1p 52	
IEEE 802.1Q 47	
IEEE 802.1x	
IGMP 65, 95	
IGMP snooping 65, 67, 95	
IGMP Snooping 65	
Ingress filtering 48	
Invalid entry 15	
IP address 19, 54	
default 11	
IP Authorized Manager 54	
IVL 47	
1	
– LACP 61 62	
Light Beacon	
Link Laver Discovery Protocol 28	
LI DP. 28	
LLD PDUs 28	
Log 76	
M	
MAC	
MAC address 20, 78	
MAC errors	
Management Information Base	
MD5	
Media Redundancy Protocol See MRP	
Member ports 49	
Menu tree 13	
MFB	
MID 11 25 27 05	
MDD 44	
MRP	
Multiseet 06	
Wulticast strooms	
Wultifunction Putton	
multi moster exercision	
10000-1000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-10000-1000-1000-10000-1000-	
Ν	
Network analyser 75	



HARTING

Operation sequence		12
Р		
Password		24
Pina		79
PNAC		55
Port mirroring	75.	96
Port status		43
Power over Ethernet	See F	оE
priority class		50
privilege status		26
PROFINET		86
PROFINET IO Stack		38
PVID		48
_		
Q		
QoS		96
R		
Rapid Spanning Tree Protocol	See RS	TP
Rate Control		53
Reboot	12,	37
Redundancy		40
RSTP Section		40
RFC		96
RMON		71
RSTP	40,	96
RSTP statistics		82
s		
Safety Guidelines and Approved Usage		8
Save configuration	14	20
SD card	,	44
Secure Hash Algorithm (SHA)		26
Security		54
SHA		27
SMTP		96
SMTP server		69
SNMP	11 25	96
SNMP alert	11, 20,	70
SNMPv1/v2		25
SNMPv3		25
SNTP		30
Statistics		80
STP		<u>⊿∩</u>
Subnet mask	10 20	97
S\/I	10, 20,	<u>4</u> 7
•••		-11

т

Tag Control Information See	TCI
TCI	50
TCN	43
TFTP 34	, 97
TFTP server	35
Time settings	30
ToS	50
Traffic class	52
Trap receiver	70
Trivial File Transfer ProtocolSee T	FTP
0	
Untagged ports	49
Untagged ports User Authentication	49 27
Untagged ports User Authentication User modes	49 27 16
Untagged ports User Authentication User modes User, new created	49 27 16 23
Untagged ports User Authentication User modes User, new created USM	49 27 16 23 25
Untagged ports User Authentication User modes User, new created USM	49 27 16 23 25
Untagged ports User Authentication User modes User, new created USM V VLAN	49 27 16 23 25 9, 97
Untagged ports User Authentication User modes User, new created USM V VLAN 47, 49	49 27 16 23 25 9, 97



HARTING Technology Group info@HARTING.com www.HARTING.com Version vom 10. 2013