



# **DG-IS4508HP/IS4512HP/IS4514HP**

Industrial Ethernet POE L2 SWITCHES

## **User Manual**

**V1.0**

**2016-08-20**



## User Manual

---

As our products undergo continuous development the specifications are subject to change without prior notice

## **COPYRIGHT**

Copyright 2016 by Smartlink Network Systems Ltd. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of this company.

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents thereof without obligation to notify any person of such revision or changes.

## **Trademarks:**

DIGISOL™ is a trademark of Smartlink Network Systems Ltd. All other trademarks are the property of the respective manufacturers.

## **Safety**

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

# Table of Contents

## Contents

1.	Introduction .....	14
1.1	System Description.....	14
1.2	Using the Web Interface.....	14
	<b>Web Browser Support .....</b>	<b>14</b>
	<b>Navigation .....</b>	<b>15</b>
	<b>Title Bar Icons .....</b>	<b>15</b>
	<b>Ending a Session .....</b>	<b>16</b>
	<b>Using the Online Help .....</b>	<b>16</b>
2.	Using the Web.....	17
2.1	Login.....	17
2.2	Tree View.....	18
	<b>Configuration Menu.....</b>	<b>18</b>
	<b>Monitor Menu .....</b>	<b>19</b>
	<b>Diagnostics Menu .....</b>	<b>20</b>
	<b>Maintenance Menu.....</b>	<b>20</b>
2.3	Configuration.....	21
2.3.1	System Information .....	21
2.3.2	System IP .....	22
2.3.3	System NTP .....	25



2.3.4 System Time .....	26
2.3.5 System Log .....	28
2.3.6 System Alarm Profile .....	30
2.4 Green Ethernet .....	32
2.4.1 Port Power Savings .....	32
2.4.2 Port .....	34
2.5 DHCP .....	36
2.5.1 DHCP Server .....	36
2.5.2 DHCP Snooping .....	41
2.5.3 DHCP Relay .....	42
2.6 Security .....	45
2.6.1 Switch .....	45
2.7 SNMP .....	55
2.7.1 SNMP System Configuration .....	55
2.7.2 SNMP Trap Configuration .....	57
2.7.3 SNMP Communities .....	61
2.7.4 SNMP Users .....	63
2.7.5 SNMP Groups .....	65
2.7.6 SNMP Views .....	67
2.7.7 SNMP Access .....	69
2.8 RMON .....	71
2.8.1 RMON Statistics .....	71

2.8.2 RMON History .....	72
2.8.3 RMON Alarm .....	74
2.8.4 RMON Event.....	76
2.8.5 Network .....	78
ACL Port .....	93
IP Source Guard Configuration.....	108
Port Configuration .....	111
VLAN Configuration .....	113
Static Table.....	115
Dynamic Table .....	116
2.8.6 AAA.....	118
RADIUS .....	118
TACACS+ .....	121
2.9 Aggregation .....	123
2.9.1 Static Aggregation .....	123
2.9.2 LACP Aggregation.....	125
2.9.3 Loop Protection .....	127
3.0 Spanning Tree .....	129
3.0.1 Bridge Settings.....	129
3.0.2 MSTI Mapping .....	131
3.0.3 MSTI Priorities .....	133
3.0.4 CIST Ports .....	135

3.0.5 MSTI Ports.....	138
3.1 IPMC Profile.....	141
3.1.1 Profile Table.....	141
3.1.2 Address Entry.....	143
3.2 MVR .....	145
3.3 IPMC .....	148
3.3.1 IGMP Snooping .....	148
3.3.2 MLD Snooping .....	155
Basic Configuration.....	155
VLAN Configuration .....	157
Port Filtering Profile .....	160
3.4 LLDP .....	161
3.4.1 LLDP .....	161
3.4.2 LLDP-MED .....	163
3.5 PoE .....	170
3.5.1 PoE Scheduler.....	172
3.5.2 Power Reset .....	173
3.5.3 MAC Table .....	175
3.5.4 VLANs.....	176
3.6 Private VLANs .....	181
3.6.1 Membership .....	181
3.6.2 Port Isolation.....	184

3.7 VCL .....	186
3.7.1 MAC-based VLAN.....	186
3.7.2 Protocol-based VLAN .....	188
Protocol to Group.....	188
3.7.3 Group to VLAN .....	190
3.7.4 IP Subnet-based VLAN .....	192
3.8 Voice VLAN .....	193
3.8.1 Voice VLAN Configuration .....	193
3.8.2 Voice VLAN OUI .....	196
3.9 QoS .....	197
3.9.1 Port Classification.....	197
3.9.2 Port Policing .....	200
3.9.3 Port Scheduler.....	202
3.9.4 Port Shaping.....	203
3.9.5 Port Tag Remarking .....	204
3.9.6 Port DSCP.....	205
3.9.7 DSCP-Based QoS .....	207
3.9.8 DSCP Translation .....	209
3.9.9 DSCP Classification.....	211
3.9.10 QoS Control List.....	212
3.9.11 Storm Control .....	217
4.0 Mirroring .....	219

5.0 GVRP.....	221
5.1 Global Config .....	221
5.2 Port Config .....	222
6.0 sFlow .....	222
7.0 RingV2.....	226
8.0 DDM.....	229
<b>Monitor.....</b>	<b>230</b>
<b>System .....</b>	<b>230</b>
<b>System Information .....</b>	<b>230</b>
<b>CPU Load .....</b>	<b>232</b>
<b>IP Status .....</b>	<b>233</b>
<b>System Log.....</b>	<b>235</b>
<b>System Detailed Log .....</b>	<b>237</b>
<b>System Alarm .....</b>	<b>238</b>
<b>Green Ethernet .....</b>	<b>239</b>
<b>Port Power Saving .....</b>	<b>239</b>
<b>Ports .....</b>	<b>240</b>
<b>Ports State .....</b>	<b>240</b>
<b>Trafice Overview.....</b>	<b>241</b>
<b>QoS Statistics .....</b>	<b>242</b>
<b>QCL Status.....</b>	<b>243</b>
<b>Detailed Statistics .....</b>	<b>245</b>

<b>DHCP .....</b>	<b>247</b>
<b>DHCP Server .....</b>	<b>247</b>
<b>Statistics .....</b>	<b>247</b>
<b>Binding .....</b>	<b>249</b>
<b>Declined IP .....</b>	<b>251</b>
<b>DHCP Snooping Table .....</b>	<b>252</b>
<b>DHCP Relay Statistics .....</b>	<b>254</b>
<b>DHCP Detailed Statistics.....</b>	<b>256</b>
<b>Security .....</b>	<b>258</b>
<b>Accessment Management Statistics .....</b>	<b>258</b>
<b>Network .....</b>	<b>259</b>
<b>Port Security .....</b>	<b>259</b>
<b>Switch .....</b>	<b>259</b>
<b>Port .....</b>	<b>262</b>
<b>NAS.....</b>	<b>264</b>
<b>Switch .....</b>	<b>264</b>
<b>Port .....</b>	<b>266</b>
<b>ACL Status.....</b>	<b>269</b>
<b>ARP Inspection.....</b>	<b>271</b>
<b>IP Source Guard .....</b>	<b>273</b>
<b>AAA.....</b>	<b>275</b>
<b>RADIUS Overview .....</b>	<b>275</b>

<b>RADIUS Details</b> .....	277
<b>Switch</b> .....	278
<b>RMON</b> .....	278
<b>Statistics</b> .....	278
<b>History</b> .....	280
<b>Alarm</b> .....	282
<b>Event</b> .....	283
<b>LACP</b> .....	285
<b>System Status</b> .....	285
<b>Port Status</b> .....	286
<b>Port Statistics</b> .....	287
<b>Loop Protection</b> .....	289
<b>Spanning Tree</b> .....	290
<b>Bridge Status</b> .....	290
<b>Port Status</b> .....	291
<b>Port Statistics</b> .....	292
<b>MVR</b> .....	293
<b>MVR Statistics</b> .....	293
<b>MVR Channel Groups</b> .....	295
<b>MVR SFM Information</b> .....	297
<b>IPMC</b> .....	299
<b>IGMP Snooping</b> .....	299

<b>IGMP Snooping Status .....</b>	<b>299</b>
<b>Groups Information .....</b>	<b>301</b>
<b>IPv4 SFM Information .....</b>	<b>303</b>
<b>MLD Snooping .....</b>	<b>305</b>
<b>MLD Snooping Status .....</b>	<b>305</b>
<b>Groups Information .....</b>	<b>307</b>
<b>IPv6 SFM Information .....</b>	<b>309</b>
<b>LLDP .....</b>	<b>311</b>
<b>Neighbors .....</b>	<b>311</b>
<b>LLDP-MED Neighbors .....</b>	<b>313</b>
<b>EEE .....</b>	<b>318</b>
<b>Port Statistics .....</b>	<b>320</b>
<b>PoE .....</b>	<b>322</b>
<b>MAC Table .....</b>	<b>324</b>
<b>VLANs .....</b>	<b>326</b>
<b>VLANs Membership .....</b>	<b>326</b>
<b>VLANs Ports .....</b>	<b>328</b>
<b>VCL .....</b>	<b>330</b>
<b>MAC-Based VLAN .....</b>	<b>330</b>
<b>sFlow .....</b>	<b>331</b>
<b>RingV2 .....</b>	<b>333</b>
<b>DDMI Overview .....</b>	<b>334</b>



<b>DDMI Detailed .....</b>	<b>334</b>
<b>Diagnostics.....</b>	<b>336</b>
<b>Ping.....</b>	<b>336</b>
<b>Ping6 .....</b>	<b>338</b>
<b>VeriPHY .....</b>	<b>340</b>
<b>Maintenance.....</b>	<b>342</b>
<b>Restart Device .....</b>	<b>342</b>
<b>Factory Default .....</b>	<b>343</b>
<b>Software .....</b>	<b>344</b>
<b>Software Upload.....</b>	<b>344</b>
<b>Image select .....</b>	<b>345</b>
<b>Configuration .....</b>	<b>347</b>
<b>Save startup-config .....</b>	<b>347</b>
<b>Download .....</b>	<b>348</b>
<b>Upload.....</b>	<b>349</b>
<b>Activate.....</b>	<b>350</b>
<b>Delete .....</b>	<b>351</b>

# 1. Introduction

## 1.1 System Description

DIGISOL Bolt Series industrial Ethernet switches delivers high quality, wide operating temperature range, extended power input range, IP-30 design, and advanced VLAN & QoS features. It's ideal for harsh environments and mission critical applications.

Managed QoS provides enterprise-class networking features to fulfill the needs of large network infrastructure and extreme environments.

DG-IS4508HP/IS4512HP/IS4514HP eases the effort to build a network infrastructure which offers a reliable, well managed and good QoS networking for any business requiring continuous and well-protected services in management environments. With the features such as Fast Failover ring protection and QoS, customers can ensure their network is qualified to deliver any real-time and high quality applications.

## 1.2 Using the Web Interface

The object of this document “DG-IS4508HP/IS4512HP/IS4514HP Web Configuration Tool Guide” is to address the web feature, design layout and describe how to use the web interface. The GUI snapshots and features may differ from actual product.

The Default IP address of switch is 192.0.2.1/24.

## Web Browser Support

IE 7 (or newer version) with the following default settings is recommended:

Language script	Latin based
Web page font	Times New Roman
Plain text font	Courier New
Encoding	Unicode (UTF-8)
Text size	Medium

Firefox with the following default settings is recommended:

Web page font	Times New Roman
Encoding	Unicode (UTF-8)
Text size	16

Google Chrome with the following default settings is recommended:

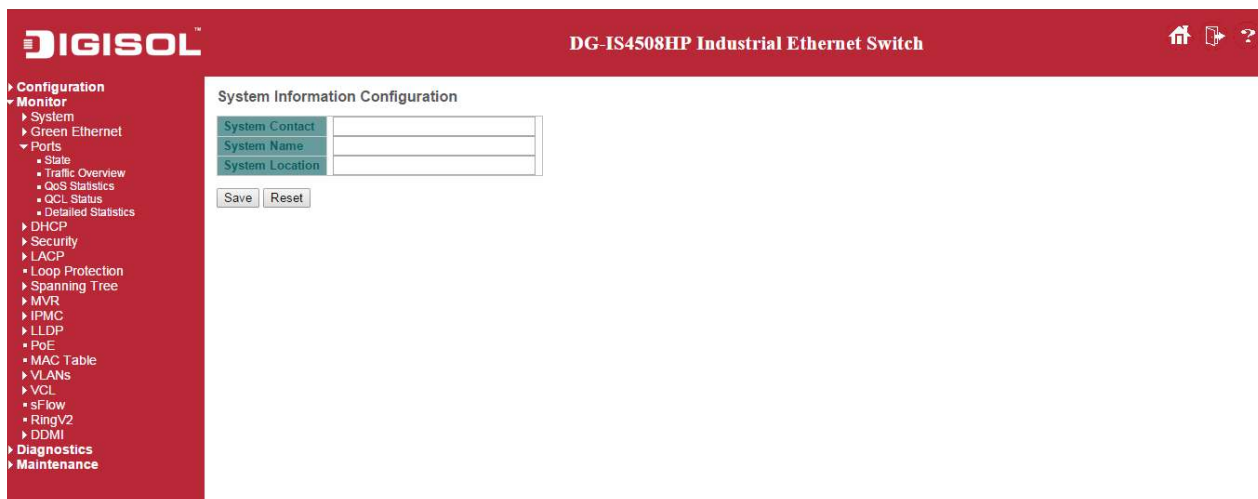
Web page font	Times New Roman
Encoding	Unicode (UTF-8)
Text size	Medium

## Navigation

All main screens of the web interface can be reached by clicking on hyperlinks in the four menu boxes on the left side of the screen:

- **Configuration**
- **Monitor**
- **Diagnostics**
- **Maintenance**

## Title Bar Icons

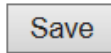


**Help Button**



For more information about any screen, click on the Help button on the screen.  
Help information is displayed in the same window.

### Save Button



If any unsaved change has been made to the *configuration* (by you during this or a prior session, or by any other administrator using the web interface or the Command Line Interface), a Save icon appears in the title line. To save the running configuration to the startup configuration:


1. Click on the Save icon. The System/Save and Restore screen appears.
2. Click on Submit next to Data Control Action drop-down list on top of System/Save and Restore screen.

## Ending a Session

To end a session, close your web browser. This prevents an unauthorized user from accessing the system using your user name and password.

## Using the Online Help



Each screen has a  Help button that invokes a page of information relevant to the particular screen. The Help is displayed in a new window.

Each web page of Configuration/Status/System functions has a corresponding help page.

## 2. Using the Web

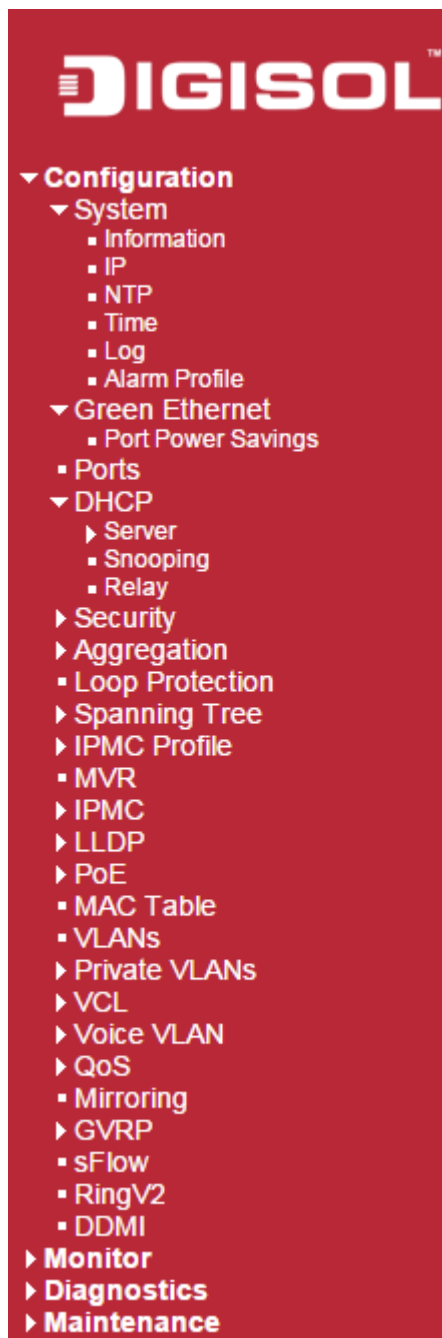
### 2.1 Login

<b>Operation</b>	1. Fill Username and Password 2. Click "Sign in"
<b>Field</b>	Description
<b>Username</b>	Login user name. The maximum length is 32. Default: admin
<b>Password</b>	Login user password. The maximum length is 32. Default: none

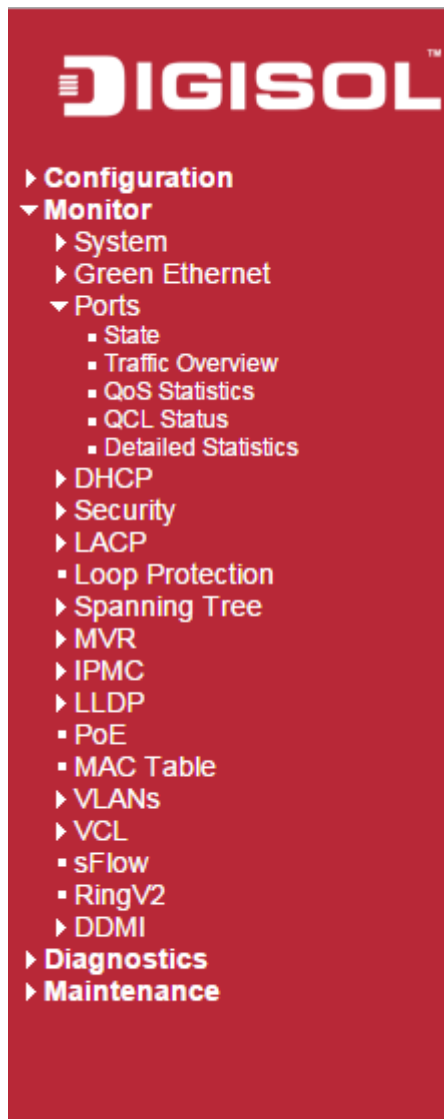
## 2.2 Tree View

The tree view is a menu of the web. It offers user quickly to get the page for expected data or configuration.

### Configuration Menu



## Monitor Menu



## Diagnostics Menu



## Maintenance Menu





## 2.3 Configuration

### 2.3.1 System Information

The switch system information is provided here.

**DIGISOL™** DG-IS4508HP Industrial Ethernet Switch

**Configuration**

- System
  - Information
  - IP
  - NTP
  - Time
  - Log
  - Alarm Profile
- Green Ethernet
  - Port Power Savings
- Ports
- DHCP
  - Server
  - Snooping
  - Relay
- Security
- Aggregation
- Loop Protection
- Spanning Tree

**System Information Configuration**

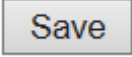
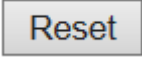
System Contact

System Name

System Location

Save Reset

Object	Description
<b>System Contact</b>	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
<b>System Name</b>	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
<b>System Location</b>	The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

Buttons	
	Click to save changes.
	Click to revert to previously saved values.

## 2.3.2 System IP

Configure [IP](#) basic settings, control IP interfaces and IP routes.

The maximum number of interfaces supported is 8 and the maximum number of routes is 32.

**DIGISOL™** **DG-IS4508HP Industrial Ethernet Switch**

**Configuration**

- System
  - Information
  - IP
  - NTP
  - Time
  - Log
  - Alarm Profile
- Green Ethernet
  - Port Power Savings
- Ports
- DHCP
  - Server
  - Snooping
  - Relay
- Security
  - Aggregation
  - Loop Protection
  - Spanning Tree
  - IPMC Profile
  - MVR
  - IPMC
  - LLDP
  - PoE
  - MAC Table
  - VLANs
  - Private VLANs
  - VCL
  - Voice VLAN
  - QoS
  - Mirroring
  - GVRP

**IP Configuration**

Mode: Host  
 DNS Server: No DNS server  
 DNS Proxy: ☐

**IP Interfaces**

Delete	VLAN	Enable	Fallback	Current Lease	IPv4 Address	Mask Length	IPv6 Address	Mask Length
<input type="checkbox"/>	1	<input type="checkbox"/>	0		192.0.2.1	24		

Add Interface

**Default Gateway**

Address:

Set Default Gateway

**IP Routes**

Delete	Network	Mask Length	Gateway	Next Hop VLAN
--------	---------	-------------	---------	---------------

Add Route

Save Reset

Object	Description
<b>IP Configuration</b>	
<b>Mode</b>	Configure whether the IP stack should act as a <b>Host</b> or a <b>Router</b> . In <b>Host</b> mode, IP traffic between interfaces will not be routed. In <b>Router</b> mode traffic is routed between all interfaces.
<b>DNS Server</b>	<p>This setting controls the DNS name resolution done by the switch. The following modes are supported:</p> <ul style="list-style-type: none"> <li><b>From any DHCP interfaces</b></li> </ul> <p>The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used.</p>

	<ul style="list-style-type: none"> <li>• <b>No DNS server</b>  No DNS server will be used.</li> <li>• <b>Configured</b>  Explicitly provide the IP address of the DNS Server in <a href="#">dotted decimal notation</a>.</li> <li>• <b>From this DHCP interface</b>  Specify from which DHCP-enabled interface a provided DNS server should be preferred.</li> </ul>
<b>DNS Proxy</b>	When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network.
<b>IP Interfaces</b>	
<b>Delete</b>	Select this option to delete an existing IP interface.
<b>VLAN</b>	The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.
<b>IPv4 DHCP Enabled</b>	Enable the DHCP client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCP protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
<b>IPv4 DHCP Fallback Timeout</b>	The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.
<b>IPv4 DHCP Current Lease</b>	For DHCP interfaces with an active lease, this column show the current interface address, as provided by the DHCP server.
<b>IPv4 Address</b>	The IPv4 address of the interface in <a href="#">dotted decimal notation</a> .  If <b>DHCP</b> is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.
<b>IPv4 Mask</b>	The IPv4 network mask, in number of bits ( <i>prefix length</i> ). Valid values are between 0 and 30 bits for a IPv4 address.

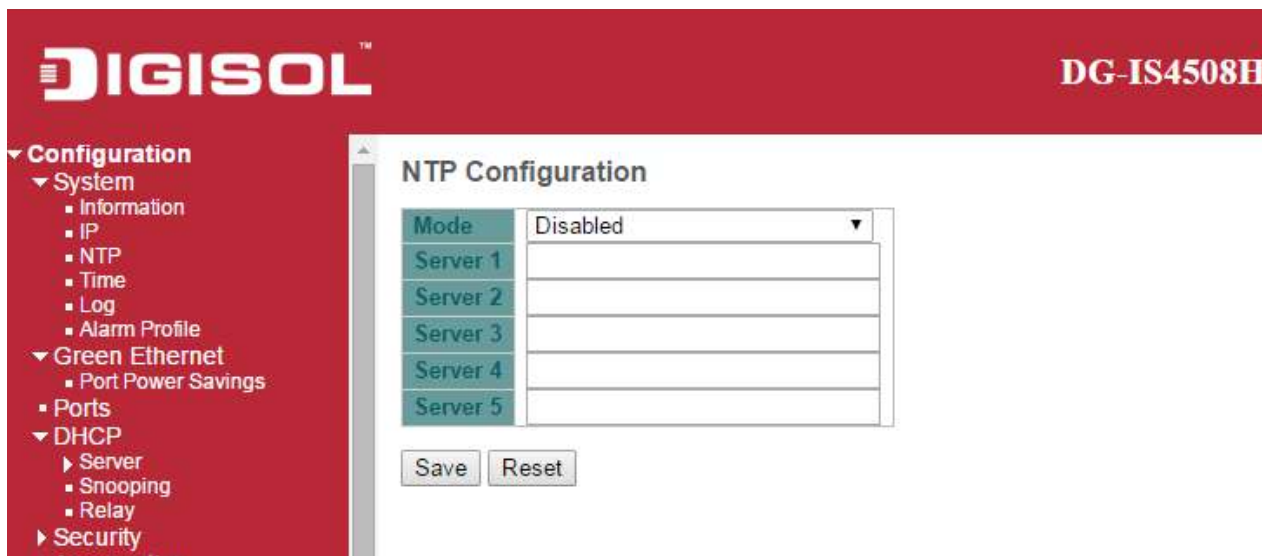
	If <b>DHCP</b> is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.
<b>IPv6 Address</b>	<p>The IPv6 address of the interface. A IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, <b>fe80::215:c5ff:fe03:4dc7</b>. The symbol <b>::</b> is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, <b>::192.1.2.34</b>.</p> <p>The field may be left blank if IPv6 operation on the interface is not desired.</p>
<b>IPv6 Mask</b>	<p>The IPv6 network mask, in number of bits (<i>prefix length</i>). Valid values are between 1 and 128 bits for a IPv6 address.</p> <p>The field may be left blank if IPv6 operation on the interface is not desired.</p>
<b>Default Gateway</b>	
<b>Address</b>	The IP address of the gateway valid format is <a href="#">dotted decimal notation</a> .
<b>IP Routes</b>	
<b>Delete</b>	Select this option to delete an existing IP route.
<b>Network</b>	<p>The destination IP network or host address of this route. Valid format is <a href="#">dotted decimal notation</a> or a valid IPv6 notation. A default route can use the value <b>0.0.0.0</b> or IPv6 <b>::</b> notation.</p>
<b>Mask Length</b>	<p>The destination IP network or host mask, in number of bits (<i>prefix length</i>). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of <b>0</b> (as it will match anything).</p>
<b>Gateway</b>	The IP address of the IP gateway. Valid format is <a href="#">dotted decimal notation</a> or a valid IPv6 notation. Gateway and Network must be of the same type.
<b>Next Hop VLAN(Only for IPv6)</b>	<p>The VLAN ID (VID) of the specific IPv6 interface associated with the gateway. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.</p> <p>If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway.</p> <p>If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.</p>

## Buttons

<b>Add Interface</b>	Click to add a new IP interface. A maximum of 8 interfaces is supported.
<b>Set Default Gateway</b>	Click to save changes.
<b>Add Route</b>	Click to add a new IP route. A maximum of 32 routes is supported.
<b>Save</b>	Click to save changes.
<b>Reset</b>	Click to revert to previously saved values.

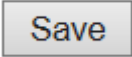
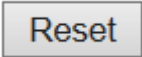
### 2.3.3 System NTP

Configure NTP on this page.



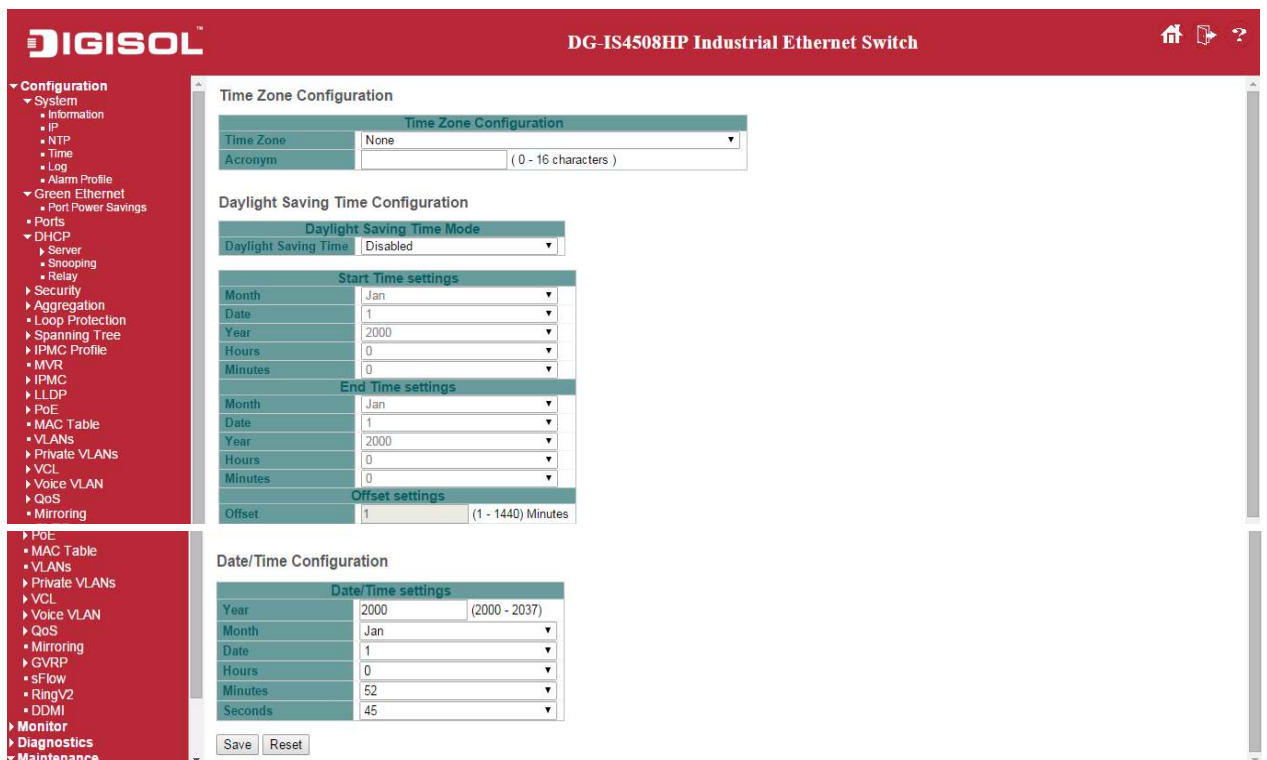
Object	Description
<b>Mode</b>	Indicates the NTP mode operation. Possible modes are: <b>Enabled:</b> Enable NTP client mode operation. <b>Disabled:</b> Disable NTP client mode operation.
<b>Server #</b>	Provide the IPv4 or IPv6 address of a NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating

	each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
--	--

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## 2.3.4 System Time

This page allows you to configure the Time Zone

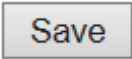
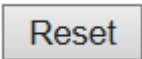


The screenshot shows the DIGISOL web interface for the DG-IS4508HP Industrial Ethernet Switch. The left sidebar contains a navigation menu with categories like Configuration, Monitor, Diagnostics, and Maintenance. The main content area is titled 'Time Zone Configuration' and includes sections for 'Time Zone Configuration', 'Daylight Saving Time Configuration', and 'Date/Time Configuration'. The 'Time Zone Configuration' section has dropdowns for 'Time Zone' (set to 'None') and 'Acronym' (with a character limit of 16). The 'Daylight Saving Time Configuration' section has a 'Daylight Saving Time Mode' dropdown (set to 'Disabled') and 'Start Time settings' (Month: Jan, Date: 1, Year: 2000, Hours: 0, Minutes: 0) and 'End Time settings' (Month: Jan, Date: 1, Year: 2000, Hours: 0, Minutes: 0). The 'Date/Time Configuration' section has 'Date/Time settings' (Year: 2000, Month: Jan, Date: 1, Hours: 0, Minutes: 52, Seconds: 45) and 'Offset settings' (Offset: 1, with a range of 1 - 1440 minutes). At the bottom of the configuration area are 'Save' and 'Reset' buttons.

Object	Description
Time Zone Configuration	

<b>Time Zone</b>	Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Save to set.
<b>Acronym</b>	User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. ( Range : Up to 16 characters )
<b>Daylight Saving Time Configuration</b>	
<b>Daylight Saving Time</b>	This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. ( Default : Disabled )
<b>Recurring Configurations</b>	
<b>Start time settings</b>	
<b>Week</b>	Select the starting week number.
<b>Day</b>	Select the starting day.
<b>Month</b>	Select the starting month.
<b>Hours</b>	Select the starting hour.
<b>Minutes</b>	Select the starting minute
<b>End time settings</b>	
<b>Week</b>	Select the ending week number.
<b>Day</b>	Select the ending day.
<b>Month</b>	Select the ending month.
<b>Hours</b>	Select the ending hour.
<b>Minutes</b>	Select the ending minute
<b>Offset settings</b>	
<b>Offset</b>	Enter the number of minutes to add during Daylight Saving Time. ( Range: 1 to 1440 )
<b>Non Recurring Configurations</b>	
<b>Start time settings</b>	
<b>Month</b>	Select the starting month.
<b>Date</b>	Select the starting date.
<b>Year</b>	Select the starting year.
<b>Hours</b>	Select the starting hour.
<b>Minutes</b>	Select the starting minute
<b>End time settings</b>	
<b>Month</b>	Select the ending month.

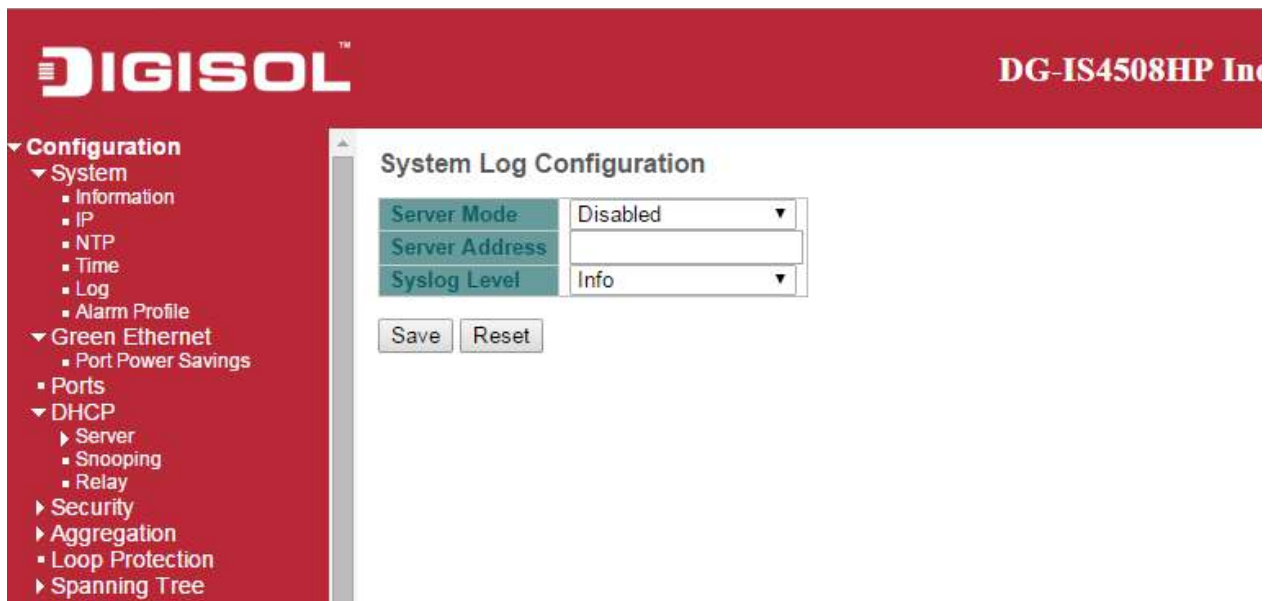
<b>Date</b>	Select the ending date.
<b>Year</b>	Select the ending year.
<b>Hours</b>	Select the ending hour.
<b>Minutes</b>	Select the ending minute
<b>Offset settings</b>	
<b>Offset</b>	Enter the number of minutes to add during Daylight Saving Time. ( Range: 1 to 1440 )
<b>Date/Time Configuration</b>	
<b>Date/Time Settings</b>	
<b>Year</b>	Year of current datetime. ( Range: 2000 to 2037 )
<b>Month</b>	Month of current datetime.
<b>Date</b>	Date of current datetime.
<b>Hours</b>	Hour of current datetime.
<b>Minutes</b>	Minute of current datetime.
<b>Seconds</b>	Second of current datetime.

<b>Buttons</b>	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

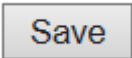
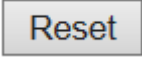
### 2.3.5 System Log

Configure System Log on this page.



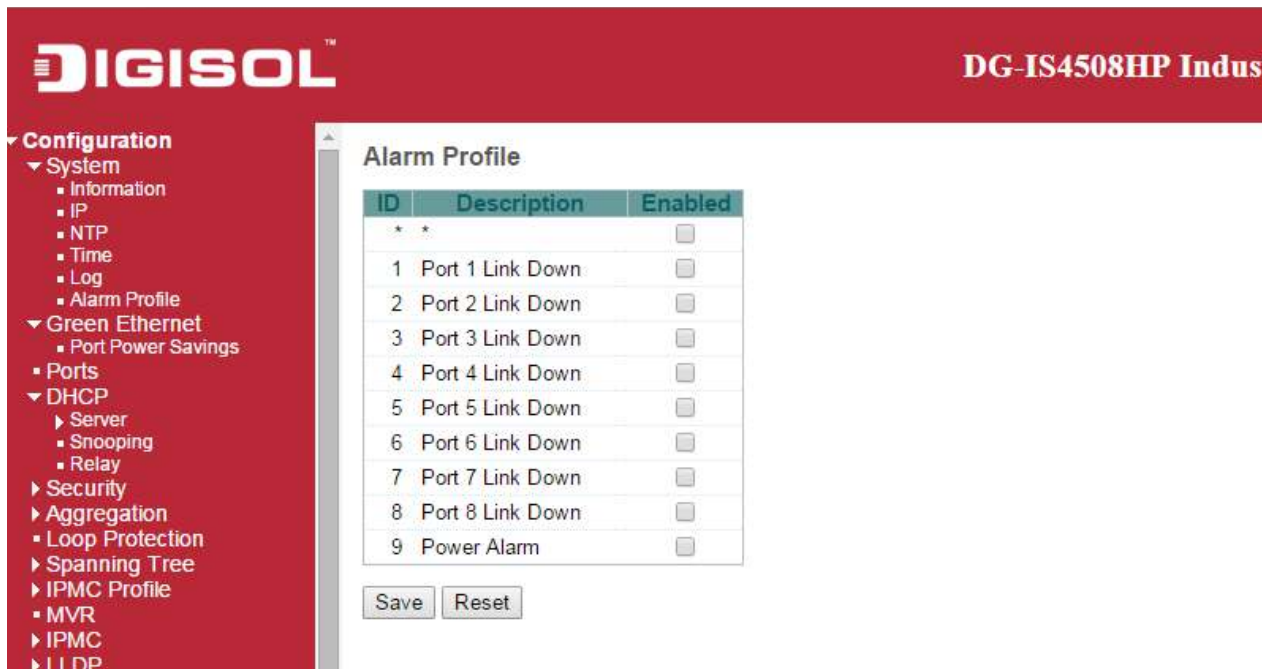


Object	Description
<b>Server Mode</b>	Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are: <b>Enabled:</b> Enable server mode operation. <b>Disabled:</b> Disable server mode operation.
<b>Server Address</b>	Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a host name.
<b>Syslog Level</b>	Indicates what kind of message will send to syslog server. Possible modes are: <b>Info:</b> Send informations, warnings and errors. <b>Warning:</b> Send warnings and errors. <b>Error:</b> Send errors.

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

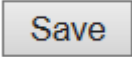
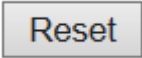
### 2.3.6 System Alarm Profile

Alarm Profile is provided here to enable/disable alarm



Object	Description
<b>ID</b>	The identification of the Alarm Profile entry.
<b>Description</b>	Alarm Type Description.
<b>Enabled</b>	<p>If alarm entry is Enabled, then alarm will be shown in alarm history/current when it occurs.</p> <p>Alarm LED will be on (lighted), Alarm Relay also be enabled.</p> <p>SNMP trap will be sent if any SNMP trap entry exists and enabled.</p>
<b>Disabled</b>	<p>If alarm entry is Disabled, then alarm will not be captured/shown in alarm history/current when alarm occurs;</p> <p>then it will not trigger the Alarm LED change, Alarm Relay and SNMP trap either.</p>
<p>Note: When any alarm exists, the Alarm LED will be on (lighted), Alarm Output Relay will also be enabled.</p>	

#### Buttons

	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## 2.4 Green Ethernet

### 2.4.1 Port Power Savings

This page allows the user to configure the port power savings features.

**DIGISOL™** DG-IS4508HP Industrial Ethernet Switch

**Configuration**

- System
- Green Ethernet
  - Port Power Savings
- Ports
- DHCP
  - Server
  - Snooping
  - Relay
- Security
- Aggregation
- Loop Protection
- Spanning Tree
- IPMC Profile
  - MVR
- IPMC
- LLDP
- PoE
  - MAC Table
- VLANs
  - Private VLANs
- VCL
- Voice VLAN
- QoS
- Mirroring

**Port Power Savings Configuration**

Optimize EEE for: Latency

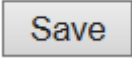
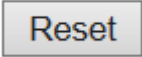
**Port Configuration**

Port	ActiPHY	PerfectReach	EEE	EEE Urgent Queues									
				1	2	3	4	5	6	7	8		
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save Reset

Object	Description
<b>Port Power Savings Configuration</b>	
<b>Optimize EEE for</b>	The switch can be set to optimize EEE for either best power saving or least traffic latency.
<b>Port Configuration</b>	
<b>Port</b>	The switch port number of the logical port.
<b>ActiPHY</b>	<p>Link down power savings enabled.</p> <p>ActiPHY works by lowering the power for a port when there is no link. The port is power up for short moment in order to determine if cable is inserted.</p>
<b>PerfectReach</b>	<p>Cable length power savings enabled.</p> <p>PerfectReach works by determining the cable length and lowering the power for ports</p>

	with short cables.
<b>EEE</b>	<p>Controls whether <a href="#">EEE</a> is enabled for this switch port.</p> <p>For maximizing power savings, the circuit isn't started at once transmit data is ready for a port, but is instead queued until a burst of data is ready to be transmitted. This will give some traffic latency.</p> <p>If desired it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.</p>
<b>EEE Urgent Queues</b>	<p>Queues set will activate transmission of frames as soon as data is available.</p> <p>Otherwise the queue will postpone transmission until a burst of frames can be transmitted.</p>

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## 2.4.2 Port

This page displays current port configurations. Ports can also be configured here.

**DIGISOL** DG-IS4508HP Industrial Ethernet Switch

**Configuration**

- System
- Green Ethernet
- Ports
- DHCP
  - Server
  - Snooping
  - Relay
- Security
- Aggregation
- Loop Protection
- Spanning Tree
- IPMC Profile
  - MVR
  - IPMC
  - LLDP
- PoE
  - MAC Table
  - VLANs
  - Private VLANs
  - VCL
  - Voice VLAN
  - QoS
  - Mirroring
  - GVRP
  - sFlow
  - PortVLAN

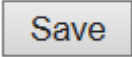
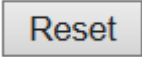
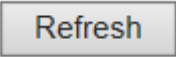
**Port Configuration**

Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode
		Current	Configured	Current Rx	Current Tx	Configured		
*			<>				9600	<>
1	Down	Auto	Auto	X	X		9600	Discard
2	Down	Auto	Auto	X	X		9600	Discard
3	Down	Auto	Auto	X	X		9600	Discard
4	Down	Auto	Auto	X	X		9600	Discard
5	1Gfdx	Auto	Auto	X	X		9600	Discard
6	Down	Auto	Auto	X	X		9600	Discard
7	Down	Auto	Auto	X	X		9600	
8	Down	Auto	Auto	X	X		9600	

Save Reset

Object	Description
<b>Port</b>	This is the logical port number for this row.
<b>Link</b>	The current link state is displayed graphically. Green indicates the link is up and red that it is down.
<b>Current Link Speed</b>	Provides the current link speed of the port.
<b>Configured Link Speed</b>	<p>Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are:</p> <p><b>Disabled</b> - Disables the switch port operation.</p> <p><b>Auto</b> - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner.</p> <p><b>10Mbps HDX</b> - Forces the cu port in 10Mbps half duplex mode.</p> <p><b>10Mbps FDX</b> - Forces the cu port in 10Mbps full duplex mode.</p> <p><b>100Mbps HDX</b> - Forces the cu port in 100Mbps half duplex mode.</p> <p><b>100Mbps FDX</b> - Forces the cu port in 100Mbps full duplex mode.</p> <p><b>1Gbps FDX</b> - Forces the port in 1Gbps full duplex .</p>
<b>Flow Control</b>	When <b>Auto Speed</b> is selected on a port, this section indicates the flow control

	<p>capability that is advertised to the link partner.</p> <p>When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last <a href="#">Auto-Negotiation</a>.</p> <p>Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.</p>
<b>Maximum Frame Size</b>	Enter the maximum frame size allowed for the switch port, including FCS.
<b>Excessive Collision Mode</b>	<p>Configure port transmit collision behavior.</p> <p><b>Discard:</b> Discard frame after 16 collisions (default).</p> <p><b>Restart:</b> Restart backoff algorithm after 16 collisions.</p>

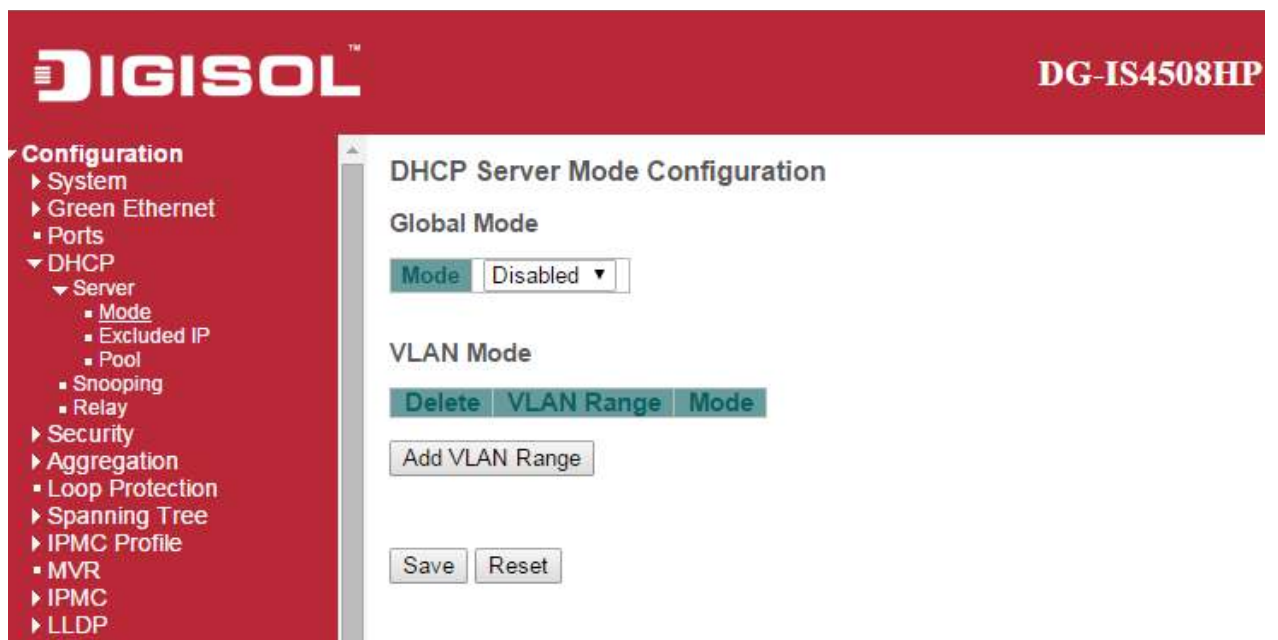
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.
	Click to refresh the page. Any changes made locally will be undone.

## 2.5 DHCP

### 2.5.1 DHCP Server

#### DHCP Server Mode



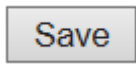
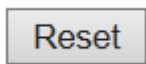
This page configures global mode and VLAN mode to enable/disable DHCP server per system and per VLAN.



Object	Description
<b>Global Mode</b>	
<b>Mode</b>	Configure the operation mode per system. Possible modes are: <b>Enabled:</b> Enable DHCP server per system. <b>Disabled:</b> Disable DHCP server per system.
<b>VLAN Mode</b>	
<b>VLAN Range</b>	Indicate the VLAN range in which DHCP server is enabled or disabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. BUT, if the VLAN range contains only 1 VLAN ID, then you can just input it into either one of the first and

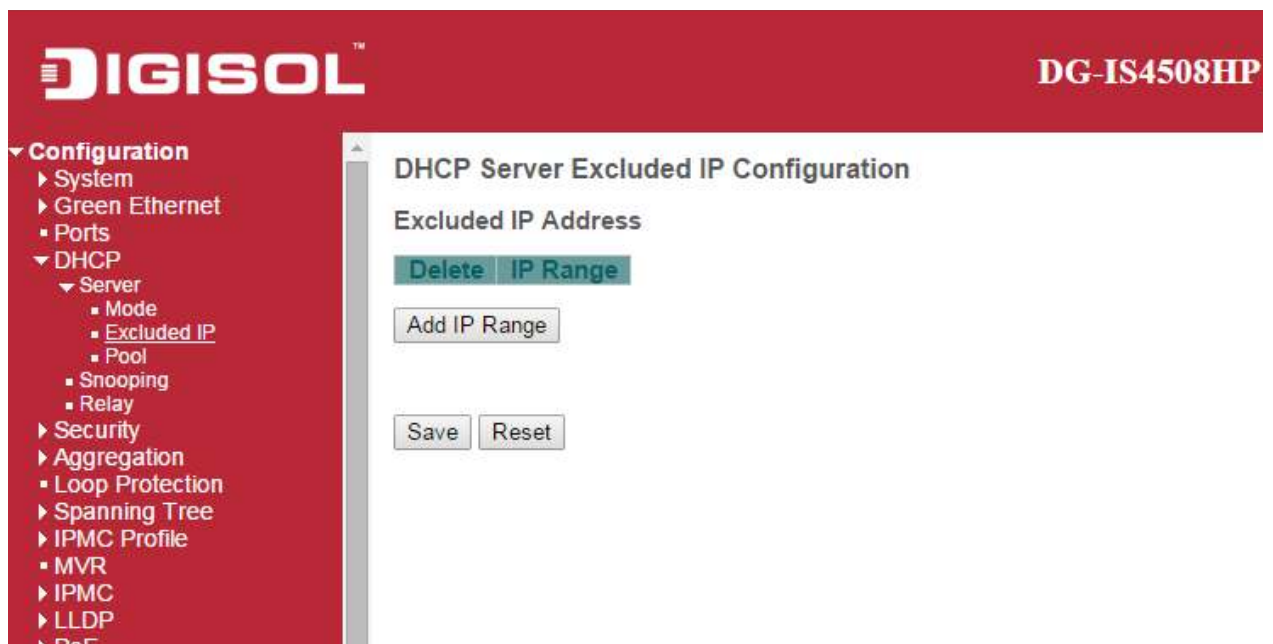


	<p>second VLAN ID or both.</p> <p>On the other hand, if you want to disable existed VLAN range, then you can follow the steps.</p> <ol style="list-style-type: none"> <li>1. press to add a new VLAN range.</li> <li>2. input the VLAN range that you want to disable.</li> <li>3. choose Mode to be <b>Disabled</b>.</li> <li>4. press to apply the change.</li> </ol> <p>Then, you will see the disabled VLAN range is removed from the DHCP Server mode configuration page.</p>
<b>Mode</b>	<p>Indicate the the operation mode per VLAN. Possible modes are:</p> <p><b>Enabled</b>: Enable DHCP server per VLAN.</p> <p><b>Disabled</b>: Disable DHCP server pre VLAN.</p>



Buttons	
	Click to delete the setting.
	Click to add a new VLAN range.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

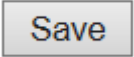
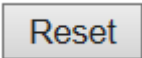
## DHCP Server Excluded IP

This page configures excluded IP addresses. DHCP server will not allocate these excluded IP addresses to DHCP client.



Object	Description
<b>IP Range</b>	Define the IP range to be excluded IP addresses. The first excluded IP must be smaller than or equal to the second excluded IP. BUT, if the IP range contains only 1 excluded IP, then you can just input it to either one of the first and second excluded IP or both.

Buttons	
	Click to delete the setting.
	Click to add a new excluded IP range.

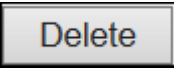

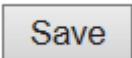
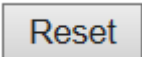
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## DHCP Server Pool

This page manages DHCP pools. According to the DHCP pool, DHCP server will allocate IP address and deliver configuration parameters to DHCP client.

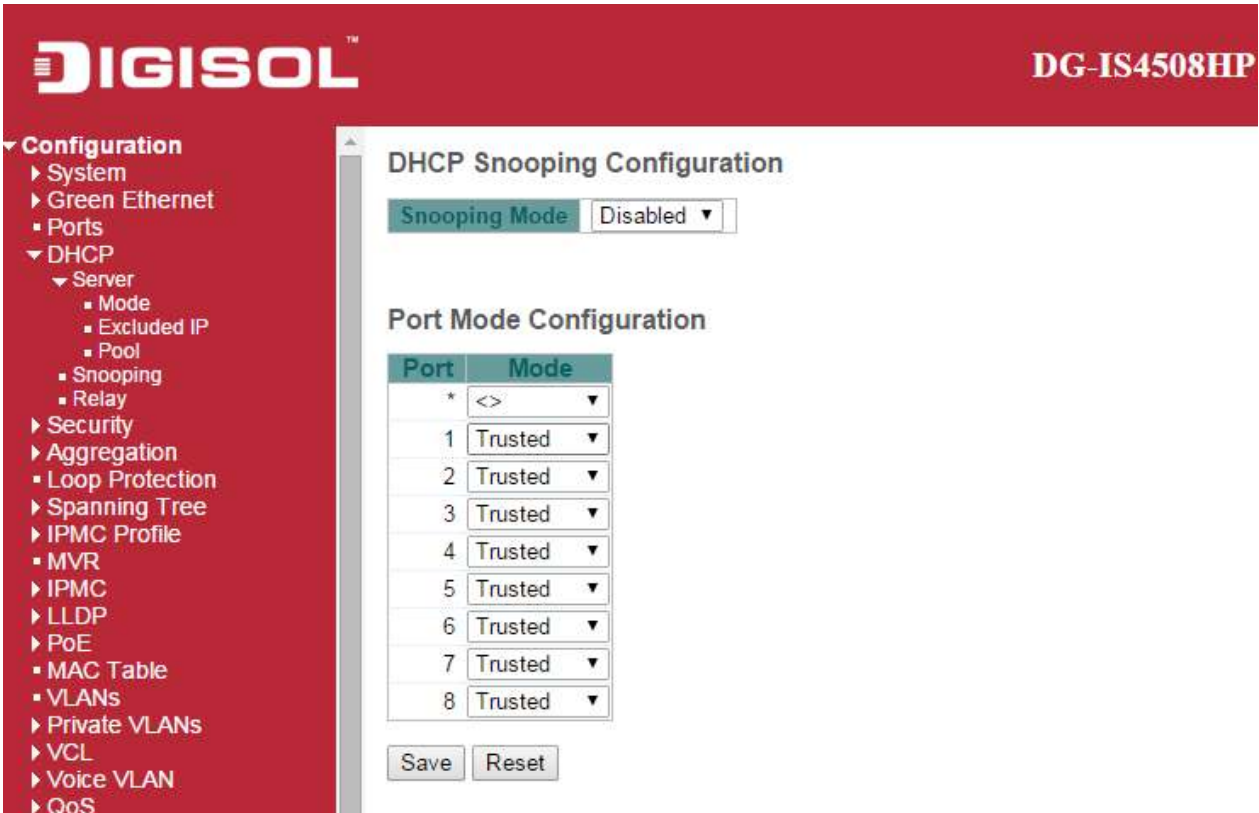


Object	Description
<b>Name</b>	Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page.
<b>Type</b>	<p>Display which type of the pool is.</p> <p><b>Network</b>: the pool defines a pool of IP addresses to service more than one DHCP client.</p> <p><b>Host</b>: the pool services for a specific DHCP client identified by client identifier or hardware address.</p> <p>If "-" is displayed, it means not defined.</p>
<b>IP</b>	<p>Display network number of the DHCP address pool.</p> <p>If "-" is displayed, it means not defined.</p>
<b>Subnet Mask</b>	<p>Display subnet mask of the DHCP address pool.</p> <p>If "-" is displayed, it means not defined.</p>
<b>Lease Time</b>	Display lease time of the pool.

Buttons	
	Click to delete the setting.
	Click to add a new DHCP pool.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## 2.5.2 DHCP Snooping

Configure DHCP Snooping on this page.



**DIGISOL™** **DG-IS4508HP**

**Configuration**

- System
- Green Ethernet
- Ports
- DHCP**
  - Server
    - Mode
    - Excluded IP
    - Pool
  - Snooping
  - Relay
- Security
- Aggregation
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- PoE
- MAC Table
- VLANs
- Private VLANs
- VCL
- Voice VLAN
- QoS

**DHCP Snooping Configuration**

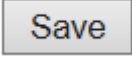
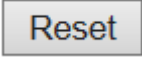
Snooping Mode: Disabled

**Port Mode Configuration**

Port	Mode
*	<>
1	Trusted
2	Trusted
3	Trusted
4	Trusted
5	Trusted
6	Trusted
7	Trusted
8	Trusted

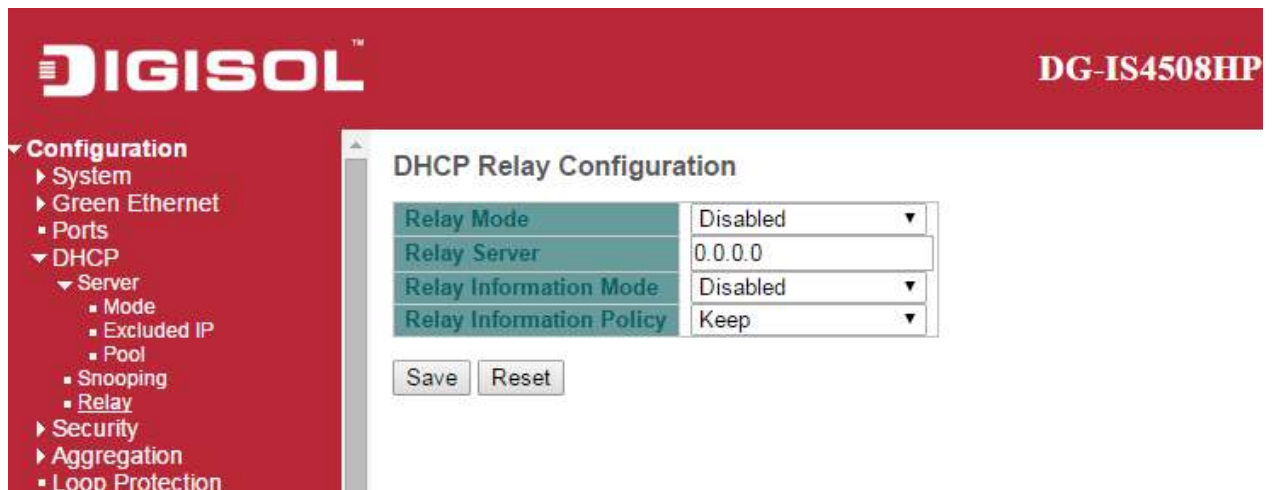
Save Reset

Object	Description
<b>Snooping Mode</b>	Indicates the DHCP snooping mode operation. Possible modes are: <b>Enabled</b> : Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports. <b>Disabled</b> : Disable DHCP snooping mode operation.
<b>Port Mode Configuration</b>	Indicates the DHCP snooping port mode. Possible port modes are: <b>Trusted</b> : Configures the port as trusted source of the DHCP messages. <b>Untrusted</b> : Configures the port as untrusted source of the DHCP messages.

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

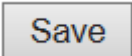
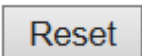
### 2.5.3 DHCP Relay

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such condition, please make sure the switch configuration of VLAN interface IP address and PVID(Port VLAN ID) correctly.



Object	Description
<b>Relay Mode</b>	<p>Indicates the DHCP relay mode operation.</p> <p>Possible modes are:</p> <p><b>Enabled:</b> Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.</p> <p><b>Disabled:</b> Disable DHCP relay mode operation.</p>
<b>Relay Server</b>	Indicates the DHCP relay server <a href="#">IP</a> address.
<b>Relay Information Mode</b>	<p>Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID(in standalone device it always equal 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.</p> <p>Possible modes are:</p> <p><b>Enabled:</b> Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.</p> <p><b>Disabled:</b> Disable DHCP relay information mode operation.</p>

<b>Relay Information Policy</b>	<p>Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are:</p> <p><b>Replace:</b> Replace the original relay information when a DHCP message that already contains it is received.</p> <p><b>Keep:</b> Keep the original relay information when a DHCP message that already contains it is received.</p> <p><b>Drop:</b> Drop the package when a DHCP message that already contains relay information is received.</p>
---------------------------------	--

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.



## 2.6 Security

### 2.6.1 Switch


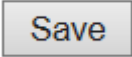
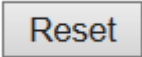
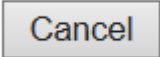
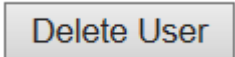
#### Users

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.

The screenshot shows the DIGISOL DG-IS4508HP web interface. On the left is a navigation menu under 'Configuration' with options like System, Green Ethernet, Ports, DHCP, Security, and Switch. The 'Security' > 'Switch' > 'Users' path is highlighted. The main content area is titled 'Add User' and contains a 'User Settings' form. The form has four input fields: 'User Name', 'Password', 'Password (again)', and 'Privilege Level' (which is a dropdown menu currently showing '1'). Below the form are three buttons: 'Save', 'Reset', and 'Cancel'.


Object	Description
<b>User Name</b>	A string identifying the user name that this entry should belong to. The allowed string length is <b>1</b> to <b>31</b> . The valid user name allows letters, numbers and underscores.
<b>Password</b>	The password of the user. The allowed string length is <b>0</b> to <b>31</b> . Any printable characters including space is accepted.
<b>Privilege Level</b>	The privilege level of the user. The allowed range is <b>1</b> to <b>15</b> . If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload,

	factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.
--	--

Buttons	
	Click to add a new user.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.
	Click to undo any changes made locally and return to the Users.
	Delete the current user. This button is not available for new configurations (Add new user)

## Privilege Level

This page provides an overview of the privilege levels.



**DG-IS4508HP Industrial Ethernet Switch**

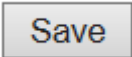
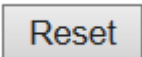
- Configuration
  - System
  - Green Ethernet
  - Ports
  - DHCP
  - Security
    - Switch
      - Users
      - Privilege Levels
      - Auth Method
      - SSH
      - HTTPS
      - Access Management
      - SNMP
      - RMON
    - Network
    - AAA
  - Aggregation
  - Loop Protection
  - Spanning Tree
  - IPMC Profile
  - MVR
  - IPMC
  - LLDP
  - PoE
    - MAC Table
    - VLANs
  - Private VLANs
  - VCL
  - Voice VLAN
  - QoS
    - Mirroring
  - GVRP
  - sFlow
  - RingV2
  - DDMI
- Monitor
- Diagnostics
  - POE
    - MAC Table
    - VLANs
  - Private VLANs
  - VCL
  - Voice VLAN
  - QoS
    - Mirroring
  - GVRP
  - sFlow
  - RingV2
  - DDMI

### Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5 ▼	10 ▼	5 ▼	10 ▼
Debug	15 ▼	15 ▼	15 ▼	15 ▼
DHCP	5 ▼	10 ▼	5 ▼	10 ▼
Dhcp_Client	5 ▼	10 ▼	5 ▼	10 ▼
Diagnostics	5 ▼	10 ▼	5 ▼	10 ▼
EEE	5 ▼	10 ▼	5 ▼	10 ▼
Green_Ethernet	5 ▼	10 ▼	5 ▼	10 ▼
IP2	5 ▼	10 ▼	5 ▼	10 ▼
IPMC_Snooping	5 ▼	10 ▼	5 ▼	10 ▼
LACP	5 ▼	10 ▼	5 ▼	10 ▼
LLDP	5 ▼	10 ▼	5 ▼	10 ▼
Loop_Protect	5 ▼	10 ▼	5 ▼	10 ▼
MAC_Table	5 ▼	10 ▼	5 ▼	10 ▼
Maintenance	15 ▼	15 ▼	15 ▼	15 ▼
Mirroring	5 ▼	10 ▼	5 ▼	10 ▼
MVR	5 ▼	10 ▼	5 ▼	10 ▼
NTP	5 ▼	10 ▼	5 ▼	10 ▼
POE	5 ▼	10 ▼	5 ▼	10 ▼
Ports	5 ▼	10 ▼	1 ▼	10 ▼
Private_VLANs	5 ▼	10 ▼	5 ▼	10 ▼
QoS	5 ▼	10 ▼	5 ▼	10 ▼
RPC	5 ▼	10 ▼	5 ▼	10 ▼
Security	5 ▼	10 ▼	5 ▼	10 ▼
sFlow	5 ▼	10 ▼	5 ▼	10 ▼
Spanning_Tree	5 ▼	10 ▼	5 ▼	10 ▼
System	5 ▼	10 ▼	1 ▼	10 ▼
Timer	5 ▼	10 ▼	5 ▼	10 ▼
VCL	5 ▼	10 ▼	5 ▼	10 ▼
VLANs	5 ▼	10 ▼	5 ▼	10 ▼
Voice_VLAN	5 ▼	10 ▼	5 ▼	10 ▼
XXRP	5 ▼	10 ▼	5 ▼	10 ▼

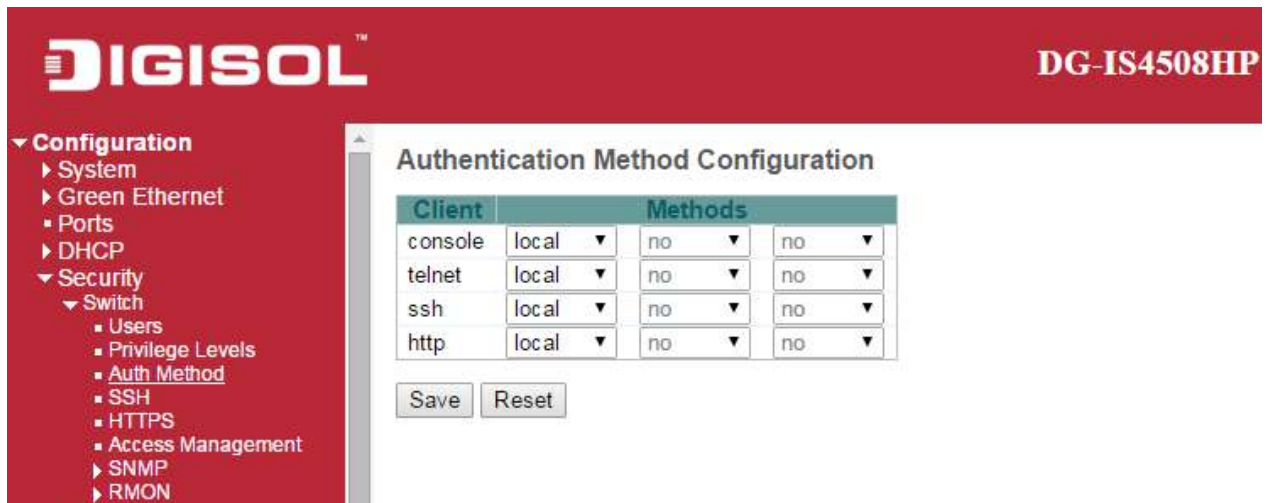
Object	Description
<b>Group Name</b>	<p>The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details:</p> <p>System: Contact, Name, Location, Timezone, Daylight Saving Time, Log.</p> <p>Security: Authentication, System Access Management, Port (contains Dot1x port,</p>

	<p>MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.</p> <p>IP: Everything except 'ping'.</p> <p>Port: Everything except 'VeriPHY'.</p> <p>Diagnostics: 'ping' and 'VeriPHY'.</p> <p>Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.</p> <p>Debug: Only present in CLI.</p>
<b>Privilege Levels</b>	<p>Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (e.g. for clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.</p>

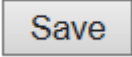
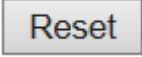
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## Auth Method

This page allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.

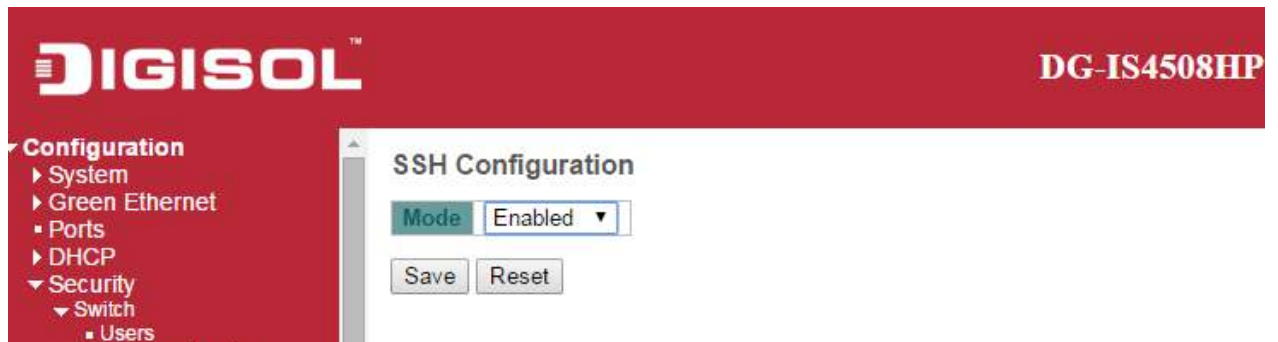


Object	Description
<b>Client</b>	The management client for which the configuration below applies.
<b>Methods</b>	<p>Method can be set to one of the following values:</p> <ul style="list-style-type: none"> <li>no: Authentication is disabled and login is not possible.</li> <li>local: Use the local user database on the switch for authentication.</li> <li>radius: Use remote <a href="#">RADIUS</a> server(s) for authentication.</li> <li>tacacs+: Use remote <a href="#">TACACS+</a> server(s) for authentication.</li> </ul> <p>Methods that involves remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.</p>

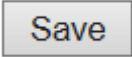
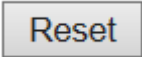
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## SSH

Configure SSH on this page.



Object	Description
<b>Mode</b>	Indicates the SSH mode operation. Possible modes are: <b>Enabled</b> : Enable SSH mode operation. <b>Disabled</b> : Disable SSH mode operation.

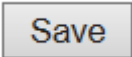
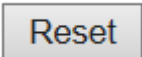
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## HTTPS

Configure HTTPS on this page.



Object	Description
<b>Mode</b>	Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. Possible modes are: <b>Enabled:</b> Enable HTTPS mode operation. <b>Disabled:</b> Disable HTTPS mode operation.
<b>Automatic Redirect</b>	Indicates the HTTPS redirect mode operation. It only significant if HTTPS mode "Enabled" is selected. Automatically redirects web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled. Possible modes are: <b>Enabled:</b> Enable HTTPS redirect mode operation. <b>Disabled:</b> Disable HTTPS redirect mode operation.

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.




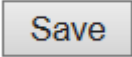
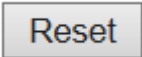
## Access Management

Configure access management table on this page. The maximum number of entries is **16**. If the application's type match any one of the access management entries, it will allow access to the switch.



Object	Description
<b>Mode</b>	Indicates the access management mode operation. Possible modes are: <b>Enabled</b> : Enable access management mode operation. <b>Disabled</b> : Disable access management mode operation.
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>VLAN ID</b>	Indicates the VLAN ID for the access management entry.
<b>Start IP address</b>	Indicates the start IP address for the access management entry.
<b>End IP address</b>	Indicates the end IP address for the access management entry.
<b>HTTP/HTTPS</b>	Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.
<b>SNMP</b>	Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.
<b>TELNET/SSH</b>	Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

### Buttons

	Click to add a new access management entry.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## 2.7 SNMP

### 2.7.1 SNMP System Configuration

Configure SNMP on this page.

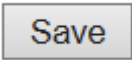
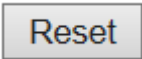
The screenshot shows the DIGISOL DG-IS4508HP web interface. On the left is a navigation menu under 'Configuration' with sub-items: System, Green Ethernet, Ports, DHCP, Security, and Switch. The 'Security' section is expanded, showing 'Switch' with sub-items: Users, Privilege Levels, Auth Method, SSH, HTTPS, and Access Management. The main content area is titled 'SNMP System Configuration'. It contains a table with the following fields:

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

Below the table are 'Save' and 'Reset' buttons.

Object	Description
<b>Mode</b>	Indicates the SNMP mode operation. Possible modes are: <b>Enabled:</b> Enable SNMP mode operation. <b>Disabled:</b> Disable SNMP mode operation.
<b>Version</b>	Indicates the SNMP supported version. Possible versions are: <b>SNMP v1:</b> Set SNMP supported version 1. <b>SNMP v2c:</b> Set SNMP supported version 2c. <b>SNMP v3:</b> Set SNMP supported version 3.
<b>Read Community</b>	Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.  The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular

	range of source addresses can be used to restrict source subnet.
<b>Write Community</b>	<p>Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.</p> <p>The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.</p>
<b>Engine ID</b>	<p>Indicates the SNMPv3 engine ID. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.</p>

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## 2.7.2 SNMP Trap Configuration

Configure SNMP trap on this page.

The screenshot shows the configuration interface for the DG-IS4508HP Industrial Ethernet Switch. The left sidebar contains a navigation tree with categories like Configuration, Security, and SNMP. The main area is titled 'SNMP Trap Configuration' and contains two sections: 'SNMP Trap Configuration' and 'SNMP Trap Event'.

**SNMP Trap Configuration**

Trap Config Name	
Trap Mode	Disabled
Trap Version	SNMP v2c
Trap Community	Public
Trap Destination Address	
Trap Destination Port	162
Trap Inform Mode	Disabled
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Probe Security Engine ID	Enabled
Trap Security Engine ID	
Trap Security Name	None

**SNMP Trap Event**

System	<input type="checkbox"/> * <input type="checkbox"/> Warm Start <input type="checkbox"/> Cold Start
Interface	Link up <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches *Link down <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches LLDP <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches
AAA	<input type="checkbox"/> * <input type="checkbox"/> Authentication Fail
Switch	<input type="checkbox"/> * <input type="checkbox"/> STP <input type="checkbox"/> RMON

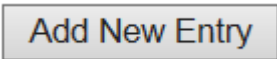
Save Reset

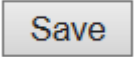
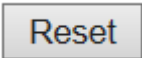
Object	Description
<b>Global Settings</b>	
<b>Mode</b>	Indicates the trap mode operation. Possible modes are: <b>Enabled:</b> Enable SNMP trap mode operation. <b>Disabled:</b> Disable SNMP trap mode operation.
<b>Trap Destination Configurations</b>	
<b>Name</b>	Indicates the trap Configuration's name. Indicates the trap destination's name.
<b>Enable</b>	Indicates the trap destination mode operation. Possible modes are: <b>Enabled:</b> Enable SNMP trap mode operation. <b>Disabled:</b> Disable SNMP trap mode operation.
<b>Version</b>	Indicates the SNMP trap supported version. Possible versions are:

	<p><b>SNMPv1</b>: Set SNMP trap supported version 1.</p> <p><b>SNMPv2c</b>: Set SNMP trap supported version 2c.</p> <p><b>SNMPv3</b>: Set SNMP trap supported version 3.</p>
<b>Destination Address</b>	<p>Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').</p> <p>And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.</p> <p>Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.</p>
<b>Destination port</b>	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

Object	Description
<b>Trap Mode</b>	<p>Indicates the SNMP trap mode operation. Possible modes are:</p> <p><b>Enabled</b>: Enable SNMP trap mode operation.</p> <p><b>Disabled</b>: Disable SNMP trap mode operation.</p>
<b>Trap Version</b>	<p>Indicates the SNMP trap supported version. Possible versions are:</p> <p><b>SNMP v1</b>: Set SNMP trap supported version 1.</p> <p><b>SNMP v2c</b>: Set SNMP trap supported version 2c.</p> <p><b>SNMP v3</b>: Set SNMP trap supported version 3.</p>
<b>Trap Community</b>	Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126.
<b>Trap Destination Address</b>	<p>Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').</p> <p>And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash</p>
<b>Trap Destination IIPv6</b>	Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records

<b>Address</b>	represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
<b>Trap Authentication Failure</b>	Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible modes are: <b>Enabled:</b> Enable SNMP trap authentication failure. <b>Disabled:</b> Disable SNMP trap authentication failure.
<b>Trap Link-up and Link-down</b>	Indicates the SNMP trap link-up and link-down mode operation. Possible modes are: <b>Enabled:</b> Enable SNMP trap link-up and link-down mode operation. <b>Disabled:</b> Disable SNMP trap link-up and link-down mode operation.
<b>Trap Inform Mode</b>	Indicates the SNMP trap inform mode operation. Possible modes are: <b>Enabled:</b> Enable SNMP trap inform mode operation. <b>Disabled:</b> Disable SNMP trap inform mode operation.
<b>Trap Inform Timeout (seconds)</b>	Indicates the SNMP trap inform timeout. The allowed range is <b>0</b> to <b>2147</b> .
<b>Trap Inform Retry Times</b>	Indicates the SNMP trap inform retry times. The allowed range is <b>0</b> to <b>255</b> .
<b>Trap Probe Security Engine ID</b>	Indicates the SNMP trap probe security engine ID mode of operation. Possible values are: <b>Enabled:</b> Enable SNMP trap probe security engine ID mode of operation. <b>Disabled:</b> Disable SNMP trap probe security engine ID mode of operation.
<b>Trap Security Engine ID</b>	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.
<b>Trap Security Name</b>	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

Buttons	
	Click to add a new user.

	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.



### 2.7.3 SNMP Communities

Configure SNMPv3 community table on this page. The entry index key is **Community**.

Object	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>Community</b>	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.
<b>Source IP</b>	Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.
<b>Source Mask</b>	Indicates the SNMP access source address mask.

Buttons	
	Click to add a new community entry.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.



## 2.7.4 SNMP Users

Configure SNMPv3 user table on this page. The entry index keys are **Engine ID** and **User Name**.

**DIGISOL™** **DG-IS4508HP Industrial Ethernet Switch**

Configuration

- System
- Green Ethernet
- Ports
- DHCP
- Security
  - Switch
    - Users
    - Privilege Levels
    - Auth Method
    - SSH
    - HTTPS
    - Access Management

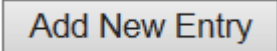
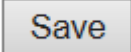
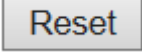
**SNMPv3 User Configuration**

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="checkbox"/>	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

Add New Entry Save Reset

Object	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>Engine ID</b>	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.
<b>User name</b>	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
<b>Security Level</b>	Indicates the security model that this entry should belong to. Possible security models are: <b>NoAuth, NoPriv</b> : No authentication and no privacy. <b>Auth, NoPriv</b> : Authentication and no privacy. <b>Auth, Priv</b> : Authentication and privacy. The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.
<b>Authentication Protocol</b>	Indicates the authentication protocol that this entry should belong to. Possible

	<p>authentication protocols are:</p> <p><b>None</b>: No authentication protocol.</p> <p><b>MD5</b>: An optional flag to indicate that this user uses MD5 authentication protocol.</p> <p><b>SHA</b>: An optional flag to indicate that this user uses SHA authentication protocol.</p> <p>The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.</p>
<b>Authentication Password</b>	A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.
<b>Privacy Protocol</b>	<p>Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:</p> <p><b>None</b>: No privacy protocol.</p> <p><b>DES</b>: An optional flag to indicate that this user uses DES authentication protocol.</p> <p><b>AES</b>: An optional flag to indicate that this user uses AES authentication protocol.</p>
<b>Privacy Password</b>	A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons	
	Click to add a new user entry.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## 2.7.5 SNMP Groups

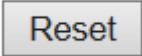
Configure SNMPv3 group table on this page. The entry index keys are **Security Model** and **Security Name**.

Delete	Security Model	Security Name	Group Name
<input type="checkbox"/>	v1	public	default_ro_group
<input type="checkbox"/>	v1	private	default_rw_group
<input type="checkbox"/>	v2c	public	default_ro_group
<input type="checkbox"/>	v2c	private	default_rw_group
<input type="checkbox"/>	usm	default_user	default_rw_group

Buttons: Add New Entry, Save, Reset

Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: <b>v1</b> : Reserved for SNMPv1. <b>v2c</b> : Reserved for SNMPv2c. <b>usm</b> : User-based Security Model (USM).
Security Name	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons	
<b>Add New Entry</b>	Click to add a new group entry
<b>Save</b>	Click to save changes.

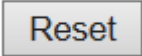
	Click to undo any changes made locally and revert to previously saved values.
---	---

## 2.7.6 SNMP Views

Configure SNMPv3 view table on this page. The entry index keys are **View Name** and **OID Subtree**.

Object	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>View Name</b>	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
<b>View Type</b>	Indicates the view type that this entry should belong to. Possible view types are: <b>included</b> : An optional flag to indicate that this view subtree should be included. <b>excluded</b> : An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.
<b>OID Subtree</b>	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

Buttons	
	Click to add a new view entry.
	Click to save changes.

	Click to undo any changes made locally and revert to previously saved values.
---	---



## 2.7.7 SNMP Access

Configure SNMPv3 access table on this page. The entry index keys are **Group Name**, **Security Model** and **Security Level**.

**DIGISOL** DG-IS4508HP Industrial Ethernet Switch

**Configuration**


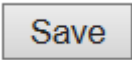
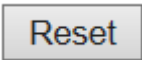
- System
- Green Ethernet
- Ports
- DHCP
- Security
  - Switch
    - Users
    - Privilege Levels
    - Auth Method
    - SSH
    - HTTPS
    - Access Management

**SNMPv3 Access Configuration**

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="checkbox"/>	default_ro_group	any	NoAuth, NoPriv	default_view ▼	None ▼
<input type="checkbox"/>	default_rw_group	any	NoAuth, NoPriv	default_view ▼	default_view ▼

Object	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>Group Name</b>	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
<b>Security Model</b>	Indicates the security model that this entry should belong to. Possible security models are: <b>any</b> : Any security model accepted(v1 v2c usm). <b>v1</b> : Reserved for SNMPv1. <b>v2c</b> : Reserved for SNMPv2c. <b>usm</b> : User-based Security Model (USM).
<b>Security Level</b>	Indicates the security model that this entry should belong to. Possible security models are: <b>NoAuth, NoPriv</b> : No authentication and no privacy. <b>Auth, NoPriv</b> : Authentication and no privacy. <b>Auth, Priv</b> : Authentication and privacy.
<b>Read View Name</b>	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
<b>Write View Name</b>	The name of the MIB view defining the MIB objects for which this request may

	potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
--	---

Buttons	
	Click to add a new access entry.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## 2.8 RMON

### 2.8.1 RMON Statistics

Configure RMON Statistics table on this page. The entry index key is **ID**.

Object	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>ID</b>	Indicates the index of the entry. The range is from 1 to 65535.
<b>Data Source</b>	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005

Buttons	
<b>Add New Entry</b>	Click to add a new community entry.
<b>Save</b>	Click to save changes.
<b>Reset</b>	Click to undo any changes made locally and revert to previously saved values.

## 2.8.2 RMON History

Configure RMON History table on this page. The entry index key is **ID**.

**DIGISOL™** DG-IS4508HP Industrial Ethernet Switch

**Configuration**

- System
- Green Ethernet
- Ports
- DHCP
- Security
  - Switch
    - Users
    - Privilege Levels
    - Auth Method
    - SSH

**RMON History Configuration**

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
Delete		1.3.6.1.2.1.2.2.1.1	0	1800	50

Object	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>ID</b>	Indicates the index of the entry. The range is from 1 to 65535.
<b>Data Source</b>	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005.
<b>Interval</b>	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
<b>Buckets</b>	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.
<b>Buckets Granted</b>	The number of data shall be saved in the RMON.

Buttons	
<input type="button" value="Add New Entry"/>	Click to add a new community entry.
<input type="button" value="Save"/>	Click to save changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.


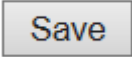
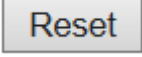


## 2.8.3 RMON Alarm

Configure RMON Alarm table on this page. The entry index key is **ID**.

Object	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>ID</b>	Indicates the index of the entry. The range is from 1 to 65
<b>Interval</b>	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to $2^{31}-1$ .
<b>Variable</b>	<p>Indicates the particular variable to be sampled, the possible variables are:</p> <p><b>InOctets</b>: The total number of octets received on the interface, including framing characters.</p> <p><b>InUcastPkts</b>: The number of uni-cast packets delivered to a higher-layer protocol.</p> <p><b>InNUcastPkts</b>: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.</p> <p><b>InDiscards</b>: The number of inbound packets that are discarded even the packets are normal.</p> <p><b>InErrors</b>: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.</p> <p><b>InUnknownProtos</b>: the number of the inbound packets that were discarded because of the unknown or un-support protocol.</p> <p><b>OutOctets</b>: The number of octets transmitted out of the interface , including framing characters.</p> <p><b>OutUcastPkts</b>: The number of uni-cast packets that request to transmit.</p>

	<p><b>OutNUcastPkts</b>: The number of broad-cast and multi-cast packets that request to transmit.</p> <p><b>OutDiscards</b>: The number of outbound packets that are discarded event the packets is normal.</p> <p><b>OutErrors</b>: The The number of outbound packets that could not be transmitted because of errors.</p> <p><b>OutQLen</b>: The length of the output packet queue (in packets).</p>
<b>Sample Type</b>	<p>The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:</p> <p><b>Absolute</b>: Get the sample directly.</p> <p><b>Delta</b>: Calculate the difference between samples (default).</p>
<b>Value</b>	The value of the statistic during the last sampling period.
<b>Startup Alarm</b>	<p>The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:</p> <p><b>Rising</b>Trigger alarm when the first value is larger than the rising threshold.</p> <p><b>Falling</b>Trigger alarm when the first value is less than the falling threshold.</p> <p><b>RisingOrFalling</b>Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).</p>
<b>Rising Threshold</b>	Rising threshold value (-2147483648-2147483647).
<b>Rising Index</b>	Rising event index (1-65535).
<b>Falling Threshold</b>	Falling threshold value (-2147483648-2147483647)
<b>Falling Index</b>	Falling event index (1-65535).

Buttons	
	Click to add a new community entry.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## 2.8.4 RMON Event

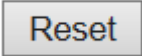
Configure RMON Event table on this page. The entry index key is **ID**.

The screenshot shows the DIGISOL web interface for the DG-IS4508HP Industrial Ethernet Switch. The left sidebar contains a navigation menu with 'Configuration' expanded, showing sub-items like System, Green Ethernet, Ports, DHCP, Security, and Switch. The main content area is titled 'RMON Event Configuration' and displays a table with the following columns: Delete, ID, Desc, Type, Community, and Event Last Time. Below the table are buttons for 'Add New Entry', 'Save', and 'Reset'.

Object	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>ID</b>	Indicates the index of the entry. The range is from 1 to 65535.
<b>Desc</b>	Indicates this event, the string length is from 0 to 127, default is a null string.
<b>Type</b>	Indicates the notification of the event, the possible types are: <b>none</b> : No SNMP log is created, no SNMP trap is sent. <b>log</b> : Create SNMP log entry when the event is triggered. <b>snmptrap</b> : Send SNMP trap when the event is triggered. <b>logandtrap</b> : Create SNMP log entry and sent SNMP trap when the event is triggered.
<b>Community</b>	Specify the community when trap is sent, the string length is from 0 to 127, default is "public".
<b>Event Last Time</b>	Indicates the value of sysUpTime at the time this event entry last generated an event.

Buttons	
<b>Add New Entry</b>	Click to add a new community entry.
<b>Save</b>	Click to save changes.



	Click to undo any changes made locally and revert to previously saved values.
---	---

## 2.8.5 Network

### Limit Control

This page allows you to configure the Port Security Limit Control system and port settings.

Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the [limit](#) specifies the maximum number of users on the port. If this number is exceeded, an [action](#) is taken. The action can be one of the four different actions as described below.

The Limit Control module utilizes a lower-layer module, Port Security module, which manages MAC addresses learnt on the port.

The Limit Control configuration consists of two sections, a system- and a port-wide.

**Port Security Limit Control Configuration**

**System Configuration**

Mode: Disabled

Aging Enabled: ☐

Aging Period: 3600 seconds

**Port Configuration**

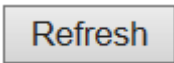
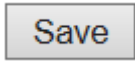
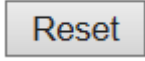
Port	Mode	Limit	Action	State	Re-open
*	<>	4	<>		
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen

Save Reset

Object	Description
--------	-------------

System Configuration	
<b>Mode</b>	Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.
<b>Aging Enabled</b>	If checked, secured MAC addresses are subject to aging as discussed under <a href="#">Aging Period</a> .
<b>Aging Period</b>	<p>If <a href="#">Aging Enabled</a> is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.</p> <p>The Aging Period can be set to a number between 10 and 10,000,000 seconds.</p> <p>To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.</p>
Port Configuration	
<b>Port</b>	The port number to which the configuration below applies.
<b>Mode</b>	Controls whether Limit Control is enabled on this port. Both this and the <a href="#">Global Mode</a> must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.
<b>Limit</b>	<p>The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding <a href="#">action</a> is taken.</p> <p>The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.</p>
<b>Action</b>	<p>If <a href="#">Limit</a> is reached, the switch can take one of the following actions:</p> <p><b>None</b>: Do not allow more than <a href="#">Limit</a> MAC addresses on the port, but take no further</p>

	<p>action.</p> <p><b>Trap:</b> If <a href="#">Limit</a> + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.</p> <p><b>Shutdown:</b> If <a href="#">Limit</a> + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:</p> <ol style="list-style-type: none"> <li>1) Boot the switch,</li> <li>2) Disable and re-enable Limit Control on the port or the switch,</li> <li>3) Click the <a href="#">Reopen</a> button.</li> </ol> <p><b>Trap &amp; Shutdown:</b> If <a href="#">Limit</a> + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.</p>
<b>State</b>	<p>This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:</p> <p><b>Disabled:</b> Limit Control is either globally disabled or disabled on the port.</p> <p><b>Ready:</b> The limit is not yet reached. This can be shown for all <a href="#">actions</a>.</p> <p><b>Limit Reached:</b> Indicates that the limit is reached on this port. This state can only be shown if <a href="#">Action</a> is set to <b>None</b> or <b>Trap</b>.</p> <p><b>Shutdown:</b> Indicates that the port is shut down by the Limit Control module. This state can only be shown if <a href="#">Action</a> is set to <b>Shutdown</b> or <b>Trap &amp; Shutdown</b>.</p>
<b>Re-open Button</b>	<p>If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to <b>Shutdown</b> in the <a href="#">Action</a> section.</p> <p>Note that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost.</p>

Buttons	
	Click to refresh the page. Note that non-committed changes will be lost.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.



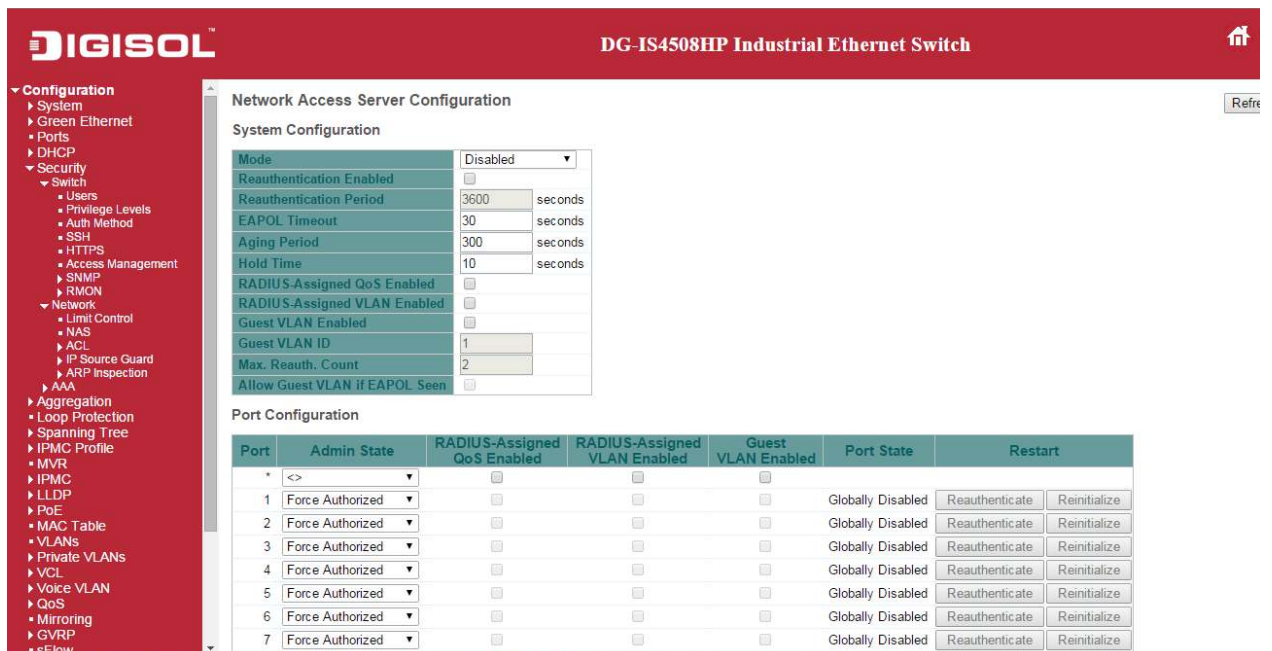
## NAS

This page allows you to configure the [IEEE 802.1X](#) and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Configuration→Security→AAA" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.

The NAS configuration consists of two sections, a system- and a port-wide.



Object	Description
<b>System Configuration</b>	
<b>Mode</b>	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.
<b>Reauthentication Enabled</b>	<p>If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.</p> <p>For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see <a href="#">Aging Period</a> below).</p>
<b>Reauthentication Period</b>	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.
<b>EAPOL Timeout</b>	<p>Determines the time for retransmission of Request Identity EAPOL frames.</p> <p>Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.</p>
<b>Aging Period</b>	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

	<ul style="list-style-type: none"> <li>• Single 802.1X</li> <li>• Multi 802.1X</li> <li>• MAC-Based Auth.</li> </ul> <p>When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.</p> <p>If <a href="#">reauthentication</a> is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.</p> <p>For ports in MAC-based Auth. mode, <a href="#">reauthentication</a> doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.</p>
<b>Hold Time</b>	<p>This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:</p> <ul style="list-style-type: none"> <li>• Single 802.1X</li> <li>• Multi 802.1X</li> <li>• MAC-Based Auth.</li> </ul> <p>If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration→Security→AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.</p> <p>In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.</p> <p>The Hold Time can be set to a number between 10 and 1000000 seconds.</p>
<b>RADIUS-Assigned QoS Enabled</b>	<p>RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see <a href="#">RADIUS-Assigned QoS Enabled</a> below for a detailed description).</p> <p>The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the</p>



	individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.
<b>RADIUS-Assigned VLAN Enabled</b>	<p>RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see <a href="#">RADIUS-Assigned VLAN Enabled</a> below for a detailed description).</p> <p>The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.</p>
<b>Guest VLAN Enabled</b>	<p>A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed <a href="#">below</a>.</p> <p>The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.</p>
<b>Guest VLAN ID</b>	<p>This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is <a href="#">globally</a> enabled.</p> <p>Valid values are in the range [1 ; 4095].</p>
<b>Max. Reauth. Count</b>	<p>The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting.</p> <p>The value can only be changed if the Guest VLAN option is <a href="#">globally</a> enabled.</p> <p>Valid values are in the range [1 ; 255].</p>
<b>Allow Guest VLAN if EAPOL Seen</b>	<p>The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port.</p>

	The value can only be changed if the Guest VLAN option is <a href="#">globally</a> enabled.
<b>Port Configuration</b>	
<b>Port</b>	The port number for which the configuration below applies.
<b>Admin State</b>	<p>If NAS is <a href="#">globally</a> enabled, this selection controls the port's authentication mode. The following modes are available:</p> <p><b>Force Authorized</b></p> <p>In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.</p> <p><b>Force Unauthorized</b></p> <p>In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.</p> <p><b>Port-based 802.1X</b></p> <p>In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (<a href="#">RFC3748</a>). Frames sent between the switch and the RADIUS server are <a href="#">RADIUS</a> packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like <a href="#">MD5-Challenge</a>, <a href="#">PEAP</a>, and <a href="#">TLS</a>. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it. When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.</p> <p><b>Note:</b> Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the</p>

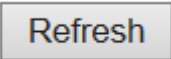
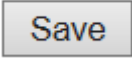
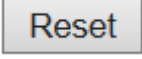
	<p>first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.</p> <p>Single 802.1X</p> <p>In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the <a href="#">Port Security</a> module is used to secure a supplicant's MAC address once successfully authenticated.</p> <p>Multi 802.1X</p> <p>Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the <a href="#">Port Security</a> module.</p> <p>In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address,</p>
--	---

	<p>which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port. The maximum number of supplicants that can be attached to a port can be limited using the <a href="#">Port Security Limit Control</a> functionality.</p> <p><b>MAC-based Auth</b></p> <p>Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the <a href="#">MD5-Challenge</a> authentication method, so the RADIUS server must be configured accordingly.</p> <p>When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the <a href="#">Port Security</a> module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the <a href="#">Port Security Limit Control</a> functionality.</p>
<p><b>RADIUS-Assigned QoS Enabled</b></p>	<p>When RADIUS-Assigned QoS is both <a href="#">globally</a> enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted</p>

	<p>to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).</p> <p>This option is only available for single-client modes, i.e.</p> <ul style="list-style-type: none"> <li>• Port-based 802.1X</li> <li>• Single 802.1X</li> </ul> <p><b><u>RADIUS attributes used in identifying a QoS Class:</u></b></p> <p>The <b>User-Priority-Table</b> attribute defined in <a href="#">RFC4675</a> forms the basis for identifying the QoS Class in an Access-Accept packet.</p> <p>Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:</p> <ul style="list-style-type: none"> <li>• All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].</li> </ul>
<b>RADIUS-Assigned VLAN Enabled</b>	<p>When RADIUS-Assigned VLAN is both <a href="#">globally</a> enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.</p> <p>If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).</p> <p>This option is only available for single-client modes, i.e.</p> <ul style="list-style-type: none"> <li>• Port-based 802.1X</li> <li>• Single 802.1X</li> </ul> <p>For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.</p> <p><b><u>RADIUS attributes used in identifying a VLAN ID:</u></b></p> <p><a href="#">RFC2868</a> and <a href="#">RFC3580</a> form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:</p> <ul style="list-style-type: none"> <li>• The <b>Tunnel-Medium-Type</b>, <b>Tunnel-Type</b>, and</li> </ul>

	<p><b>Tunnel-Private-Group-ID</b> attributes must all be present at least once in the Access-Accept packet.</p> <ul style="list-style-type: none"> <li>The switch looks for the first set of these attributes that have the same <b>Tag</b> value and fulfil the following requirements (if <b>Tag == 0</b> is used, the <b>Tunnel-Private-Group-ID</b> does not need to include a <b>Tag</b>):</li> </ul> <ul style="list-style-type: none"> <li>- Value of <b>Tunnel-Medium-Type</b> must be set to "IEEE-802" (ordinal 6).</li> <li>- Value of <b>Tunnel-Type</b> must be set to "VLAN" (ordinal 13).</li> <li>- Value of <b>Tunnel-Private-Group-ID</b> must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].</li> </ul>
<b>Guest VLAN Enabled</b>	<p>When Guest VLAN is both <a href="#">globally</a> enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.</p> <p>This option is only available for EAPOL-based modes, i.e.:</p> <ul style="list-style-type: none"> <li>Port-based 802.1X</li> <li>Single 802.1X</li> <li>Multi 802.1X</li> </ul> <p>For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.</p> <p><b><u>Guest VLAN Operation:</u></b></p> <p>When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds <a href="#">Max. Reauth. Count</a> and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with <a href="#">EAPOL Timeout</a>. If <a href="#">Allow Guest VLAN if EAPOL Seen</a> is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's <a href="#">Admin State</a> is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.</p> <p>Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.</p>

	While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.
<b>Port State</b>	<p>The current state of the port. It can undertake one of the following values:</p> <p><b>Globally Disabled:</b> NAS is <a href="#">globally</a> disabled.</p> <p><b>Link Down:</b> NAS is globally enabled, but there is no link on the port.</p> <p><b>Authorized:</b> The port is in <a href="#">Force Authorized</a> or a single-supplicant mode and the supplicant is authorized.</p> <p><b>Unauthorized:</b> The port is in <a href="#">Force Unauthorized</a> or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.</p> <p><b>X Auth/Y Unauth:</b> The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.</p>
<b>Restart</b>	<p>Two buttons are available for each row. The buttons are only enabled when authentication is <a href="#">globally enabled</a> and the port's <a href="#">Admin State</a> is in an EAPOL-based or <a href="#">MAC-based</a> mode.</p> <p>Clicking these buttons will not cause settings changed on the page to take effect.</p> <p><b>Reauthenticate:</b> Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.</p> <p>The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.</p> <p><b>Reinitialize:</b> Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.</p>

Buttons	
	Click to refresh the page. Note that non-committed changes will be lost.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.





## ACL

### ACL Port

Configure the ACL parameters ([ACE](#)) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

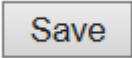
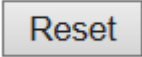

The screenshot shows the web interface for the DG-IS4508HP Industrial Ethernet Switch. The left sidebar contains a navigation tree with categories like Configuration, System, Ports, and Security. The main area is titled 'ACL Ports Configuration' and displays a table with columns: Port, Policy ID, Action, Rate Limiter ID, Port Restrict, Mirror, Logging, Shutdown, Storm, and Counter. The table lists 8 ports, each with a Policy ID of 0, Action of Permit, and Rate Limiter ID of Disabled. The Port Restrict column shows a dropdown menu with options for Port 1, Port 2, and Port 3. The Mirror, Logging, and Shutdown columns have dropdown menus with options for Disabled and Enabled. The Storm column has a dropdown menu with options for Disabled and Enabled. The Counter column shows a numerical value for each port.

Port	Policy ID	Action	Rate Limiter ID	Port Restrict	Mirror	Logging	Shutdown	Storm	Counter
1	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	2773
6	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0

Save Reset

Object	Description
<b>Port</b>	The logical port for the settings contained in the same row.
<b>Policy ID</b>	Select the policy to apply to this port. The allowed values are 0 through 255. The default value is 0.
<b>Action</b>	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
<b>Rate Limiter ID</b>	Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled".

<b>Port Redirect</b>	Select which port frames are redirected on. The allowed values are <b>Disabled</b> or a specific port number and it can't be set when action is permitted. The default value is "Disabled".
<b>Mirror</b>	Specify the mirror operation of this port. The allowed values are: <b>Enabled</b> : Frames received on the port are mirrored. <b>Disabled</b> : Frames received on the port are not mirrored. The default value is "Disabled".
<b>Loggig</b>	Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC. The allowed values are: <b>Enabled</b> : Frames received on the port are stored in the System Log. <b>Disabled</b> : Frames received on the port are not logged. The default value is "Disabled". Note: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.
<b>Shutdown</b>	Specify the port shut down operation of this port. The allowed values are: <b>Enabled</b> : If a frame is received on the port, the port will be disabled. <b>Disabled</b> : Port shut down is disabled. The default value is "Disabled". Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).
<b>State</b>	Specify the port state of this port. The allowed values are: <b>Enabled</b> : To reopen ports by changing the volatile port configuration of the ACL user module. <b>Disabled</b> : To close ports by changing the volatile port configuration of the ACL user module. The default value is "Enabled".
<b>Counter</b>	Counts the number of frames that match this ACE.

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.
	Click to refresh the page; any changes made locally will be undone.

<input type="button" value="Clear"/>	Click to clear the counters.
--------------------------------------	------------------------------

## ACL Rate Limiters

Configure the rate limiter for the [ACL](#) of the switch.

**DIGISOL** DG-IS4508HP

**Configuration**

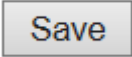
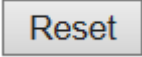
- System
- Green Ethernet
- Ports
- DHCP
- Security
  - Switch
    - Users
    - Privilege Levels
    - Auth Method
    - SSH
    - HTTPS
    - Access Management
    - SNMP
    - RMON
    - Network
      - Limit Control
      - NAS
      - ACL
        - Ports
        - Rate Limiters
        - Access Control List
      - IP Source Guard
      - ARP Inspection
    - AAA
  - Aggregation
  - Loop Protection
  - Spanning Tree
  - IPMC Profile
  - MVR
  - IPMC
  - LLDP

**ACL Rate Limiter Configuration**

Rate Limiter ID	Rate	Unit
*	1	<>
1	1	pps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

Object	Description
--------	-------------

<b>Rate Limiter ID</b>	The rate limiter ID for the settings contained in the same row.
<b>Rate</b>	The rate range is located <b>0-3276700</b> in pps. Or <b>0, 100, 200, 300, . . . , 1000000</b> in kbps.
<b>Unit</b>	Specify the rate unit. The allowed values are: <b>pps</b> : packets per second. <b>kbps</b> : Kbits per second.

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## Access Control List

This page shows the Access Control List ([ACL](#)), which is made up of the [ACEs](#) defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is **256** on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.

The screenshot shows the DIGISOL DG-IS4508HP Industrial Ethernet Switch configuration interface. The left sidebar contains a navigation tree with the following structure:

- Configuration
  - System
  - Green Ethernet
  - Ports
  - DHCP
  - Security
    - Switch
      - Users
      - Privilege Levels
      - Auth Method
      - SSH
      - HTTPS
      - Access Management
      - SNMP
      - RMON
      - Network
        - Limit Control
        - NAS
        - ACL
          - Ports
          - Rate Limiters
          - Access Control List
        - IP Source Guard
        - ARP Inspection
      - AAA

The main content area is titled "ACE Configuration". It contains the following fields:







- Ingress Port:** A dropdown menu with options: All, Port 1, Port 2, Port 3, Port 4.
- Policy Filter:** A dropdown menu with the option: Any.
- Frame Type:** A dropdown menu with the option: Any.
- Action:** A dropdown menu with the option: Permit.
- Rate Limiter:** A dropdown menu with the option: Disabled.
- Mirror:** A dropdown menu with the option: Disabled.
- Logging:** A dropdown menu with the option: Disabled.
- Shutdown:** A dropdown menu with the option: Disabled.
- Counter:** A text input field with the value: 0.

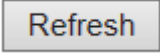
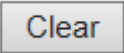
Below these fields are three buttons: Save, Reset, and Cancel.

On the right side of the interface, there is a section titled "VLAN Parameters" with the following fields:

- 802.1Q Tagged:** A dropdown menu with the option: Any.
- VLAN ID Filter:** A dropdown menu with the option: Any.
- Tag Priority:** A dropdown menu with the option: Any.

Object	Description
<b>Ingress Port</b>	Indicates the ingress port of the ACE. Possible values are: <b>All</b> : The ACE will match all ingress port. <b>Port</b> : The ACE will match a specific ingress port.
<b>Policy / Bitmask</b>	Indicates the policy number and bitmask of the ACE.
<b>Frame Type</b>	Indicates the frame type of the ACE. Possible values are: <b>Any</b> : The ACE will match any frame type. <b>EType</b> : The ACE will match <a href="#">Ethernet Type</a> frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. <b>ARP</b> : The ACE will match ARP/RARP frames. <b>IPv4</b> : The ACE will match all IPv4 frames. <b>IPv4/ICMP</b> : The ACE will match IPv4 frames with ICMP protocol.

	<p><b>IPv4/UDP:</b> The ACE will match IPv4 frames with UDP protocol.</p> <p><b>IPv4/TCP:</b> The ACE will match IPv4 frames with TCP protocol.</p> <p><b>IPv4/Other:</b> The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.</p> <p><b>IPv6:</b> The ACE will match all IPv6 standard frames.</p>
<b>Action</b>	<p>Indicates the forwarding action of the ACE.</p> <p><b>Permit:</b> Frames matching the ACE may be forwarded and learned.</p> <p><b>Deny:</b> Frames matching the ACE are dropped.</p> <p><b>Filter:</b> Frames matching the ACE are filtered.</p>
<b>Rate Limiter</b>	<p>Indicates the rate limiter number of the ACE. The allowed range is <b>1</b> to <b>16</b>. When <b>Disabled</b> is displayed, the rate limiter operation is disabled.</p>
<b>Port Redirect</b>	<p>Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are <b>Disabled</b> or a specific port number. When <b>Disabled</b> is displayed, the port redirect operation is disabled.</p>
<b>Mirror</b>	<p>Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:</p> <p><b>Enabled:</b> Frames received on the port are mirrored.</p> <p><b>Disabled:</b> Frames received on the port are not mirrored.</p> <p>The default value is "Disabled".</p>
<b>Counter</b>	<p>The counter indicates the number of times the ACE was hit by a frame.</p>
<b>Modification Buttons</b>	<p>You can modify each ACE (Access Control Entry) in the table using the following buttons:</p> <p>: Inserts a new ACE before the current row.</p> <p>: Edits the ACE row.</p> <p>: Moves the ACE up the list.</p> <p>: Moves the ACE down the list.</p> <p>: Deletes the ACE.</p> <p>: The lowest plus sign adds a new entry at the bottom of the ACE listings.</p>

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Click to refresh the page; any changes made locally will be undone.
	Click to clear the counters.

<div data-bbox="272 259 488 315" data-label="Text">Remove All</div>	Click to remove all ACEs.
---	---------------------------

Object	Description
<b>Ingress Port</b>	<p>Select the ingress port for which this ACE applies.</p> <p><b>All</b>: The ACE applies to all port.</p> <p><b>Port <i>n</i></b>: The ACE applies to this port number, where <i>n</i> is the number of the switch port.</p>
<b>Policy Filter</b>	<p>Specify the policy number filter for this ACE.</p> <p><b>Any</b>: No policy filter is specified. (policy filter status is "don't-care".)</p> <p><b>Specific</b>: If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value and bitmask appears.</p>
<b>Policy Value</b>	<p>When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is <b>0</b> to <b>255</b>.</p>
<b>Policy Bitmask</b>	<p>When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is <b>0x0</b> to <b>0xff</b>. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [policy_value &amp; policy_bitmask]. For example, if the policy value is 3 and the policy bitmask is 0x10(bit 0 is "don't-care" bit), then policy 2 and 3 are applied to this rule.</p>
<b>Frame Type</b>	<p>Select the frame type for this ACE. These frame types are mutually exclusive.</p> <p><b>Any</b>: Any frame can match this ACE.</p> <p><b>Ethernet Type</b>: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal).</p> <p><b>ARP</b>: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type.</p> <p><b>IPv4</b>: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.</p> <p><b>IPv6</b>: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.</p>
<b>Action</b>	<p>Specify the action to take with a frame that hits this ACE.</p> <p><b>Permit</b>: The frame that hits this ACE is granted permission for the ACE operation.</p> <p><b>Deny</b>: The frame that hits this ACE is dropped.</p> <p><b>Filter</b>: Frames matching the ACE are filtered.</p>

<b>Rate Limiter</b>	Specify the rate limiter in number of base units. The allowed range is <b>1</b> to <b>16</b> . <b>Disabled</b> indicates that the rate limiter operation is disabled.
<b>Port Redirect</b>	Frames that hit the ACE are redirected to the port number specified here. The rate limiter will affect these ports. The allowed range is the same as the switch port number range. <b>Disabled</b> indicates that the port redirect operation is disabled and the specific port number of 'Port Redirect' can't be set when action is permitted.
<b>Mirror</b>	Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port. The allowed values are: <b>Enabled</b> : Frames received on the port are mirrored. <b>Disabled</b> : Frames received on the port are not mirrored. The default value is "Disabled".
<b>Logging</b>	Specify the logging operation of the ACE. Notice that the logging message doesn't include the 4 bytes CRC information. The allowed values are: <b>Enabled</b> : Frames matching the ACE are stored in the System Log. <b>Disabled</b> : Frames matching the ACE are not logged. Note: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.
<b>Shutdown</b>	Specify the port shut down operation of the ACE. The allowed values are: <b>Enabled</b> : If a frame matches the ACE, the ingress port will be disabled. <b>Disabled</b> : Port shut down is disabled for the ACE. Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).
<b>Counter</b>	The counter indicates the number of times the ACE was hit by a frame.
<b>MAC Parameters</b>	
<b>SMAC Filter</b>	<i>(Only displayed when the frame type is Ethernet Type or ARP.)</i> Specify the source MAC filter for this ACE. <b>Any</b> : No SMAC filter is specified. (SMAC filter status is "don't-care".) <b>Specific</b> : If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.
<b>SMAC Value</b>	When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.
<b>DMAC Filter</b>	Specify the destination MAC filter for this ACE.



	<p><b>Any:</b> No DMAC filter is specified. (DMAC filter status is "don't-care".)</p> <p><b>MC:</b> Frame must be multicast.</p> <p><b>BC:</b> Frame must be broadcast.</p> <p><b>UC:</b> Frame must be unicast.</p> <p><b>Specific:</b> If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.</p>
<b>DMAC Value</b>	When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.
<b>VLAN Parameters</b>	
<b>802.1Q Tagged</b>	<p>Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are:</p> <p><b>Any:</b> Any value is allowed ("don't-care").</p> <p><b>Enabled:</b> Tagged frame only.</p> <p><b>Disabled:</b> Untagged frame only.</p> <p>The default value is "Any".</p>
<b>VLAN ID Filter</b>	<p>Specify the VLAN ID filter for this ACE.</p> <p><b>Any:</b> No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)</p> <p><b>Specific:</b> If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.</p>
<b>VLAN ID</b>	When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.
<b>Tag Priority</b>	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7 or range 0-1, 2-3, 4-5, 6-7, 0-3 and 4-7. The value <b>Any</b> means that no tag priority is specified (tag priority is "don't-care".)
<b>ARP Parameters</b>	
<b>ARP/RARP</b>	<p>Specify the available ARP/RARP opcode (OP) flag for this ACE.</p> <p><b>Any:</b> No ARP/RARP OP flag is specified. (OP is "don't-care".)</p> <p><b>ARP:</b> Frame must have ARP opcode set to ARP.</p> <p><b>RARP:</b> Frame must have RARP opcode set to RARP.</p> <p><b>Other:</b> Frame has unknown ARP/RARP Opcode flag.</p>
<b>Request/Reply</b>	<p>Specify the available Request/Reply opcode (OP) flag for this ACE.</p> <p><b>Any:</b> No Request/Reply OP flag is specified. (OP is "don't-care".)</p> <p><b>Request:</b> Frame must have ARP Request or RARP Request OP flag set.</p>

	<b>Reply:</b> Frame must have ARP Reply or RARP Reply OP flag.
<b>Sender IP Filter</b>	<p>Specify the sender IP filter for this ACE.</p> <p><b>Any:</b> No sender IP filter is specified. (Sender IP filter is "don't-care".)</p> <p><b>Host:</b> Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears.</p> <p><b>Network:</b> Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.</p>
<b>Sender IP Address</b>	When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in <a href="#">dotted decimal notation</a> .
<b>Sender IP Mask</b>	When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in <a href="#">dotted decimal notation</a> .
<b>Target IP Filter</b>	<p>Specify the target IP filter for this specific ACE.</p> <p><b>Any:</b> No target IP filter is specified. (Target IP filter is "don't-care".)</p> <p><b>Host:</b> Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears. <b>Network:</b> Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.</p>
<b>Target IP Address</b>	When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in <a href="#">dotted decimal notation</a> .
<b>Target IP Mask</b>	When "Network" is selected for the target IP filter, you can enter a specific target IP mask in <a href="#">dotted decimal notation</a> .
<b>ARP Sender MAC Match</b>	<p>Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.</p> <p><b>0:</b> ARP frames where SHA is not equal to the SMAC address.</p> <p><b>1:</b> ARP frames where SHA is equal to the SMAC address.</p> <p><b>Any:</b> Any value is allowed ("don't-care").</p>
<b>RARP Target MAC Match</b>	<p>Specify whether frames can hit the action according to their target hardware address field (THA) settings.</p> <p><b>0:</b> RARP frames where THA is not equal to the target MAC address.</p> <p><b>1:</b> RARP frames where THA is equal to the target MAC address.</p> <p><b>Any:</b> Any value is allowed ("don't-care").</p>
<b>IP/Ethernet Length</b>	<p>Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.</p> <p><b>0:</b> ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).</p> <p><b>1:</b> ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is</p>

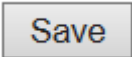
	<p>equal to IPv4 (0x04).</p> <p><b>Any:</b> Any value is allowed ("don't-care").</p>
<b>IP</b>	<p>Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.</p> <p><b>0:</b> ARP/RARP frames where the HLD is not equal to Ethernet (1).</p> <p><b>1:</b> ARP/RARP frames where the HLD is equal to Ethernet (1).</p> <p><b>Any:</b> Any value is allowed ("don't-care").</p>
<b>Ethernet</b>	<p>Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.</p> <p><b>0:</b> ARP/RARP frames where the PRO is not equal to IP (0x800).</p> <p><b>1:</b> ARP/RARP frames where the PRO is equal to IP (0x800).</p> <p><b>Any:</b> Any value is allowed ("don't-care").</p>
<b>IP Parameters</b>	
<b>IP Protocol Filter</b>	<p>Specify the IP protocol filter for this ACE.</p> <p><b>Any:</b> No IP protocol filter is specified ("don't-care").</p> <p><b>Specific:</b> If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.</p> <p><b>ICMP:</b> Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.</p> <p><b>UDP:</b> Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.</p> <p><b>TCP:</b> Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.</p>
<b>IP Protocol Value</b>	<p>When "Specific" is selected for the IP protocol value, you can enter a specific value. The allowed range is <b>0</b> to <b>255</b>. A frame that hits this ACE matches this IP protocol value.</p>
<b>IP TTL</b>	<p>Specify the Time-to-Live settings for this ACE.</p> <p><b>zero:</b> IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.</p> <p><b>non-zero:</b> IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.</p> <p><b>Any:</b> Any value is allowed ("don't-care").</p>
<b>IP Fragment</b>	<p>Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.</p> <p><b>No:</b> IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than</p>

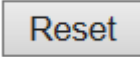

	<p>zero must not be able to match this entry.</p> <p><b>Yes:</b> IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.</p> <p><b>Any:</b> Any value is allowed ("don't-care").</p>
<b>IP Option</b>	<p>Specify the options flag setting for this ACE.</p> <p><b>No:</b> IPv4 frames where the options flag is set must not be able to match this entry.</p> <p><b>Yes:</b> IPv4 frames where the options flag is set must be able to match this entry.</p> <p><b>Any:</b> Any value is allowed ("don't-care").</p>
<b>SIP Filter</b>	<p>Specify the source IP filter for this ACE.</p> <p><b>Any:</b> No source IP filter is specified. (Source IP filter is "don't-care".)</p> <p><b>Host:</b> Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.</p> <p><b>Network:</b> Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.</p>
<b>SIP Address</b>	<p>When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in <a href="#">dotted decimal notation</a>.</p>
<b>SIP Mask</b>	<p>When "Network" is selected for the source IP filter, you can enter a specific SIP mask in <a href="#">dotted decimal notation</a>.</p>
<b>DIP Filter</b>	<p>Specify the destination IP filter for this ACE.</p> <p><b>Any:</b> No destination IP filter is specified. (Destination IP filter is "don't-care".)</p> <p><b>Host:</b> Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.</p> <p><b>Network:</b> Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.</p>
<b>DIP Address</b>	<p>When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in <a href="#">dotted decimal notation</a>.</p>
<b>DIP Mask</b>	<p>When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in <a href="#">dotted decimal notation</a>.</p>
<b>IPv6 Parameters</b>	
<b>Next Header Filter</b>	<p>Specify the IPv6 next header filter for this ACE.</p> <p><b>Any:</b> No IPv6 next header filter is specified ("don't-care").</p> <p><b>Specific:</b> If you want to filter a specific IPv6 next header filter with this ACE, choose this value. A field for entering an IPv6 next header filter appears.</p> <p><b>ICMP:</b> Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.</p> <p><b>UDP:</b> Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP</p>

	<p>parameters will appear. These fields are explained later in this help file.</p> <p><b>TCP</b>: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.</p>
<b>Next Header Value</b>	<p>When "Specific" is selected for the IPv6 next header value, you can enter a specific value. The allowed range is <b>0</b> to <b>255</b>. A frame that hits this ACE matches this IPv6 protocol value.</p>
<b>SIP Filter</b>	<p>Specify the source IPv6 filter for this ACE.</p> <p><b>Any</b>: No source IPv6 filter is specified. (Source IPv6 filter is "don't-care".)</p> <p><b>Specific</b>: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear.</p>
<b>SIP address</b>	<p>When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supported last 32 bits for IPv6 address.</p>
<b>SIP BitMask</b>	<p>When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [sipv6_address &amp; sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFF0 (bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.</p>
<b>Hop Limit</b>	<p>Specify the hop limit settings for this ACE.</p> <p><b>zero</b>: IPv6 frames with a hop limit field greater than zero must not be able to match this entry.</p> <p><b>non-zero</b>: IPv6 frames with a hop limit field greater than zero must be able to match this entry.</p> <p><b>Any</b>: Any value is allowed ("don't-care").</p>
<b>ICMP Parameters</b>	
<b>ICMP Type Filter</b>	<p>Specify the ICMP filter for this ACE.</p> <p><b>Any</b>: No ICMP filter is specified (ICMP filter status is "don't-care").</p> <p><b>Specific</b>: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.</p>
<b>ICMP Type Value</b>	<p>When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is <b>0</b> to <b>255</b>. A frame that hits this ACE matches this ICMP value.</p>
<b>ICMP Code Filter</b>	<p>Specify the ICMP code filter for this ACE.</p> <p><b>Any</b>: No ICMP code filter is specified (ICMP code filter status is "don't-care").</p> <p><b>Specific</b>: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.</p>
<b>ICMP Code Value</b>	<p>When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP</p>

	code value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value.
<b>TCP/UDP Parameters</b>	
<b>TCP/UDP Source Filter</b>	<p>Specify the TCP/UDP source filter for this ACE.</p> <p><b>Any:</b> No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care").</p> <p><b>Specific:</b> If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.</p> <p><b>Range:</b> If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.</p>
<b>TCP/UDP Source No.</b>	When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.
<b>TCP/UDP Source Range</b>	When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.
<b>TCP/UDP Destination Filter</b>	<p>Specify the TCP/UDP destination filter for this ACE.</p> <p><b>Any:</b> No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care").</p> <p><b>Specific:</b> If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.</p> <p><b>Range:</b> If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.</p>
<b>TCP/UDP Destination Number</b>	When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.
<b>TCP/UDP Destination Range</b>	When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.
<b>TCP FIN</b>	<p>Specify the TCP "No more data from sender" (FIN) value for this ACE.</p> <p><b>0:</b> TCP frames where the FIN field is set must not be able to match this entry.</p> <p><b>1:</b> TCP frames where the FIN field is set must be able to match this entry.</p>

	<b>Any:</b> Any value is allowed ("don't-care").
<b>TCP SYN</b>	Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE. <b>0:</b> TCP frames where the SYN field is set must not be able to match this entry. <b>1:</b> TCP frames where the SYN field is set must be able to match this entry. <b>Any:</b> Any value is allowed ("don't-care").
<b>TCP RST</b>	Specify the TCP "Reset the connection" (RST) value for this ACE. <b>0:</b> TCP frames where the RST field is set must not be able to match this entry. <b>1:</b> TCP frames where the RST field is set must be able to match this entry. <b>Any:</b> Any value is allowed ("don't-care").
<b>TCP PSH</b>	Specify the TCP "Push Function" (PSH) value for this ACE. <b>0:</b> TCP frames where the PSH field is set must not be able to match this entry. <b>1:</b> TCP frames where the PSH field is set must be able to match this entry. <b>Any:</b> Any value is allowed ("don't-care").
<b>TCP ACK</b>	Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE. <b>0:</b> TCP frames where the ACK field is set must not be able to match this entry. <b>1:</b> TCP frames where the ACK field is set must be able to match this entry. <b>Any:</b> Any value is allowed ("don't-care").
<b>TCP URG</b>	Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE. <b>0:</b> TCP frames where the URG field is set must not be able to match this entry. <b>1:</b> TCP frames where the URG field is set must be able to match this entry. <b>Any:</b> Any value is allowed ("don't-care").
<b>Ethernet Type Parameters</b>	
<b>EtherType Filter</b>	Specify the Ethernet type filter for this ACE. <b>Any:</b> No EtherType filter is specified (EtherType filter status is "don't-care"). <b>Specific:</b> If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering a EtherType value appears.
<b>Ethernet Type Value</b>	When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is <b>0x600</b> to <b>0xFFFF</b> but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

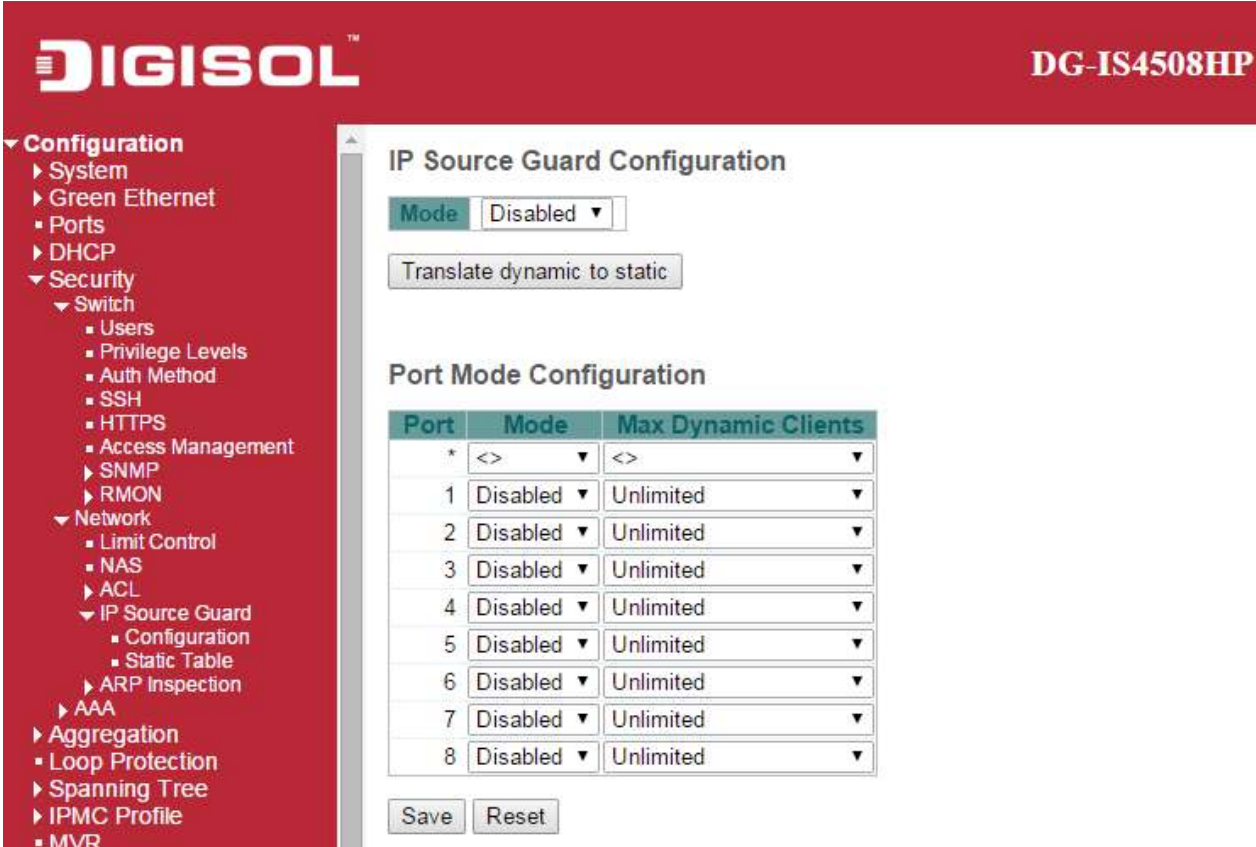
Buttons	
	Click to save changes.

	Click to undo any changes made locally and revert to previously saved values.
	Return to the previous page.

## IP Source Guard

### IP Source Guard Configuration

This page provides [IP Source Guard](#) related configuration.



**DIGISOL™** **DG-IS4508HP**

**Configuration**

- System
- Green Ethernet
- Ports
- DHCP
- Security
  - Switch
    - Users
    - Privilege Levels
    - Auth Method
    - SSH
    - HTTPS
    - Access Management
  - SNMP
  - RMON
  - Network
    - Limit Control
    - NAS
    - ACL
    - IP Source Guard
      - Configuration
      - Static Table
    - ARP Inspection
    - AAA
  - Aggregation
  - Loop Protection
  - Spanning Tree
  - IPMC Profile
  - MVR

**IP Source Guard Configuration**

Mode: Disabled

Translate dynamic to static

**Port Mode Configuration**

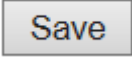
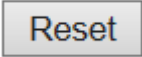
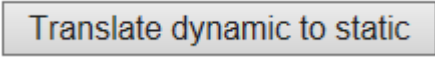
Port	Mode	Max Dynamic Clients
*	<>	<>
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited
8	Disabled	Unlimited

Save Reset

Object	Description
<b>Mode of IP Source Guard Configuration</b>	Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.
<b>Port Mode Configuration</b>	Specify IP Source Guard is enabled on which ports. Only when both Global Mode and



	Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.
<b>Max Dynamic Clients</b>	Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.
	Click to translate all dynamic entries to static entries.

## IP Source Guard Static Table

The screenshot shows the DIGISOL DG-IS4508HP configuration interface. On the left is a navigation menu with 'Configuration' expanded, showing options like System, Green Ethernet, Ports, DHCP, and Security. The 'Static IP Source Guard Table' window is open, displaying a table with columns: Delete, Port, VLAN ID, IP Address, and MAC address. The 'Delete' column has a 'Delete' button. The 'Port' column has a dropdown menu showing '1'. Below the table are buttons for 'Add New Entry', 'Save', and 'Reset'.

Object	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>Port</b>	The logical port for the settings.
<b>VLAN ID</b>	The vlan id for the settings.
<b>IP Address</b>	Allowed Source IP address.
<b>MAC address</b>	Allowed Source MAC address.

Buttons	
	Click to add a new entry to the Static IP Source Guard table.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

# ARP Inspection

## Port Configuration

This page provides [ARP Inspection](#) related configuration.

**DIGISOL™** **DG-IS4508HP**

Configuration

- System
- Green Ethernet
- Ports
- DHCP
- Security
  - Switch
    - Users
    - Privilege Levels
    - Auth Method
    - SSH
    - HTTPS
    - Access Management
    - SNMP
    - RMON
    - Network
      - Limit Control
      - NAS
      - ACL
      - IP Source Guard
        - Configuration
        - Static Table
      - ARP Inspection
        - Port Configuration
        - VLAN Configuration
        - Static Table
        - Dynamic Table
  - AAA
  - Aggregation
  - Loop Protection

**ARP Inspection Configuration**

Mode: Disabled ▼

Translate dynamic to static

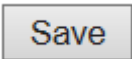
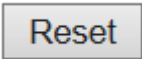
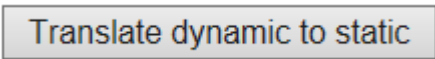
**Port Mode Configuration**

Port	Mode	Check VLAN	Log Type
*	<> ▼	<> ▼	<> ▼
1	Disabled ▼	Disabled ▼	None ▼
2	Disabled ▼	Disabled ▼	None ▼
3	Disabled ▼	Disabled ▼	None ▼
4	Disabled ▼	Disabled ▼	None ▼
5	Disabled ▼	Disabled ▼	None ▼
6	Disabled ▼	Disabled ▼	None ▼
7	Disabled ▼	Disabled ▼	None ▼
8	Disabled ▼	Disabled ▼	None ▼

Save Reset

Object	Description
<b>Mode of ARP Inspection Configuration</b>	Enable the Global ARP Inspection or disable the Global ARP Inspection.
<b>Port Mode Configuration</b>	<p>Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port.</p> <p>Possible modes are:</p> <p><b>Enabled:</b> Enable ARP Inspection operation.</p> <p><b>Disabled:</b> Disable ARP Inspection operation.</p> <p>If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of</p>

	<p>"Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are:</p> <p><b>Enabled:</b> Enable check VLAN operation.</p> <p><b>Disabled:</b> Disable check VLAN operation.</p> <p>Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and possible types are:</p> <p><b>None:</b> Log nothing.</p> <p><b>Deny:</b> Log denied entries.</p> <p><b>Permit:</b> Log permitted entries.</p> <p><b>ALL:</b> Log all entries.</p>
--	--

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.
	Click to translate all dynamic entries to static entries.

## VLAN Configuration

Each page shows up to 9999 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the closest next VLAN Table match. The will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the warning message is shown in the displayed table. Use the button to start over.

Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting.

Possible types are:

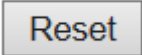
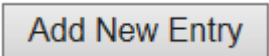
**None:** Log nothing.

**Deny:** Log denied entries.

**Permit:** Log permitted entries.

**ALL:** Log all entries

Buttons	
	Click to save changes.

	Click to undo any changes made locally and revert to previously saved values.
	Click to add a new VLAN to the ARP Inspection VLAN table.

## Static Table

**DIGISOL** DG-IS4508HP

Configuration

- System
- Green Ethernet
- Ports
- DHCP
- Security
  - Switch
    - Users
    - Privilege Levels
    - Auth Method
    - SSH
    - HTTPS

**Static ARP Inspection Table**

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1 ▼			

Add New Entry

Save Reset

Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Port	The logical port for the settings
VLAN ID	The vlan id for the settings.
MAC Address	Allowed Source MAC address in <a href="#">ARP</a> request packets.
IP Address	Allowed Source IP address in ARP request packets.

Buttons	
Add New Entry	Click to add a new entry to the Static ARP Inspection table.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

## Dynamic Table

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

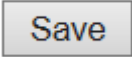
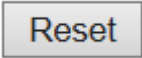
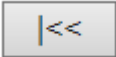

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

Object	Description
<b>Port</b>	Switch Port Number for which the entries are displayed.
<b>VLAN ID</b>	VLAN-ID in which the ARP traffic is permitted.
<b>MAC Address</b>	User MAC address of the entry.
<b>IP Address</b>	User IP address of the entry.
<b>Translate to static</b>	Select the checkbox to translate the entry to static entry.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
<input type="button" value="Refresh"/>	Refreshes the displayed table starting from the input fields.



	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.
	Updates the table starting from the first entry in the Dynamic ARP Inspection Table.
	Updates the table, starting with the entry after the last entry currently displayed.

## 2.8.6 AAA

### RADIUS

This page allows you to configure the [RADIUS](#) servers.

The screenshot shows the DIGISOL DG-IS4508HP Industrial Switch configuration interface. The left sidebar contains a navigation menu with the following structure:

- Configuration
  - System
  - Green Ethernet
  - Ports
  - DHCP
  - Security
    - Switch
      - Users
      - Privilege Levels
      - Auth Method
      - SSH
      - HTTPS
      - Access Management
    - SNMP
    - RMON
    - Network
      - Limit Control
      - NAS
      - ACL
      - IP Source Guard
        - Configuration
        - Static Table
      - ARP Inspection
        - Port Configuration
        - VLAN Configuration
        - Static Table
        - Dynamic Table

The main content area is titled "RADIUS Server Configuration". It contains two sections:

**Global Configuration**

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Key		
NAS-IP-Address		
NAS-IPv6-Address		
NAS-Identifier		

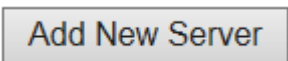

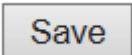
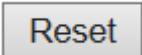
**Server Configuration**

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
Add New Server						

At the bottom of the Server Configuration section, there are "Save" and "Reset" buttons.

Object	Description
<b>Global Configuration</b>	
<b>Timeout</b>	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.
<b>Retransmit</b>	Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.
<b>Deadtime</b>	Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

	Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
<b>Key</b>	The secret key - up to 63 characters long - shared between the RADIUS server and the switch.
<b>NAS-IP-Address(Attribute 4)</b>	The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.
<b>NAS-IPv6-Address(Attribute 95)</b>	The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.
<b>NAS-Identifier (Attribute 32)</b>	The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.
<b>Server Configuration</b>	
<b>Delete</b>	To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.
<b>Hostname</b>	The IP address or hostname of the RADIUS server.
<b>Auth Port</b>	The <a href="#">UDP</a> port to use on the RADIUS server for authentication.
<b>Acct Port</b>	The <a href="#">UDP</a> port to use on the RADIUS server for accounting.
<b>Timeout</b>	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
<b>Retransmit</b>	This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.
<b>Key</b>	This optional setting overrides the global key. Leaving it blank will use the global key.

<b>Buttons</b>	
	Click to add a new RADIUS server, up to 5 servers are supported.
	The button can be used to undo the addition of the new server.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.



## TACACS+

This page allows you to configure the [TACACS+](#) servers.

**DIGISOL™** **DG-IS4508HP**

**Configuration**

- System
- Green Ethernet
- Ports
- DHCP
- Security
  - Switch
    - Users
    - Privilege Levels
    - Auth Method
    - SSH
    - HTTPS
    - Access Management
  - SNMP
  - RMON
  - Network
    - Limit Control
    - NAS
    - ACL
    - IP Source Guard

**TACACS+ Server Configuration**

**Global Configuration**

Timeout: 5 seconds

Deadtime: 0 minutes

Key:

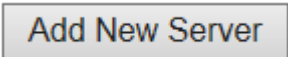

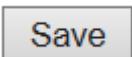
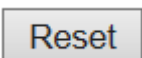
**Server Configuration**

Delete	Hostname	Port	Timeout	Key
Add New Server				

Save Reset

Object	Description
<b>Global Configuration</b>	
<b>Timeout</b>	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.
<b>Deadtime</b>	Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.  Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
<b>Key</b>	The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.
<b>Server Configuration</b>	
<b>Delete</b>	To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.
<b>Hostname</b>	The IP address or hostname of the TACACS+ server.

<b>Port</b>	The <a href="#">TCP</a> port to use on the TACACS+ server for authentication.
<b>Timeout</b>	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
<b>Key</b>	This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons	
	Click to add a new TACACS+ server, up to 5 servers are supported.
	The button can be used to undo the addition of the new server.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## 2.9 Aggregation

### 2.9.1 Static Aggregation

This page is used to configure the [Aggregation](#) hash mode and the aggregation group.

**DIGISOL™**

▼ **Configuration**

- ▶ System
- ▶ Green Ethernet
- Ports
- ▶ DHCP
- ▶ Security
- ▼ **Aggregation**
  - **Static**
  - LACP
- Loop Protection
- ▶ Spanning Tree
- ▶ IPMC Profile
- MVR
- ▶ IPMC
- ▶ LLDP
- ▶ PoE
- MAC Table
- VLANs
- ▶ Private VLANs
- ▶ VCL
- ▶ Voice VLAN
- ▶ QoS

**Aggregation Mode Configuration**

**Hash Code Contributors**

Source MAC Address	<input checked="" type="checkbox"/>
Destination MAC Address	<input type="checkbox"/>
IP Address	<input checked="" type="checkbox"/>
TCP/UDP Port Number	<input checked="" type="checkbox"/>

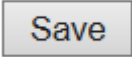
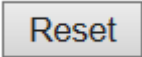
**Aggregation Group Configuration**

Group ID	Port Members							
	1	2	3	4	5	6	7	8
Normal	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Save Reset

Object	Description
<b>Hash Code Contributors</b>	
<b>Source MAC Address</b>	The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.
<b>Destination MAC Address</b>	The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to

	disable. By default, Destination MAC Address is disabled.
<b>IP Address</b>	The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.
<b>TCP/UDP Port Number</b>	The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.
<b>Aggregation Group Configuration</b>	
<b>Group ID</b>	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
<b>Port Members</b>	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.



## 2.9.2 LACP Aggregation

This page allows the user to inspect the current [LACP](#) port configurations, and possibly change them as well.

**DIGISOL™** **DG-IS4508HP Industrial**

▼ Configuration

- ▶ System
- ▶ Green Ethernet
- ▶ Ports
- ▶ DHCP
- ▶ Security
- ▼ Aggregation
  - Static
  - LACP
- Loop Protection
- ▶ Spanning Tree
- ▶ IPMC Profile
- MVR
- ▶ IPMC
- ▶ LLDP
- ▶ PoE
- MAC Table
- VLANs
- ▶ Private VLANs
- ▶ VCL

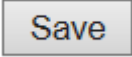
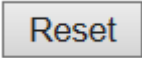
### LACP Port Configuration

Port	LACP Enabled	Key	Role	Timeout	Prio
*	<input type="checkbox"/>	<> ▼	<> ▼	<> ▼	32768
1	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768
2	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768
3	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768
4	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768
5	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768
6	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768
7	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768
8	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768

Save Reset

Object	Description
<b>Port</b>	The switch port number.
<b>LACP Enabled</b>	Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner.
<b>Key</b>	The Key value incurred by the port, range 1-65535 . The <b>Auto</b> setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the <b>Specific</b> setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
<b>Role</b>	The <b>Role</b> shows the LACP activity status. The <b>Active</b> will transmit LACP packets each second, while <b>Passive</b> will wait for a LACP packet from a partner (speak if spoken to).
<b>Timeout</b>	The <b>Timeout</b> controls the period between BPDU transmissions. <b>Fast</b> will transmit LACP packets each second, while <b>Slow</b> will wait for 30 seconds before sending a

	LACP packet.
<b>Prio</b>	The <b>Prio</b> controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

### 2.9.3 Loop Protection

This page allows the user to inspect the current Loop Protection configurations, and possibly change them as well.

**DIGISOL™** **DG-IS4508HP**

▼ **Configuration**

- ▶ System
- ▶ Green Ethernet
- ▶ Ports
- ▶ DHCP
- ▶ Security
- ▼ **Aggregation**
  - Static
  - LACP
- **Loop Protection**
- ▶ Spanning Tree
- ▶ IPMC Profile
- MVR
- ▶ IPMC
- ▶ LLDP
- ▶ PoE
- MAC Table
- VLANs
- ▶ Private VLANs
- ▶ VCL
- ▶ Voice VLAN
- ▶ QoS
- Mirroring
- ▶ GVRP
- sFlow
- RingV2
- DDMI
- ▶ **Monitor**
- ▶ **Diagnostics**

#### Loop Protection Configuration

**General Settings**

Global Configuration		
Enable Loop Protection	Disable ▼	
Transmission Time	5	seconds
Shutdown Time	180	seconds

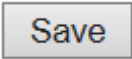

**Port Configuration**

Port	Enable	Action	Tx Mode
*	<input checked="" type="checkbox"/>	<> ▼	<> ▼
1	<input checked="" type="checkbox"/>	Shutdown Port ▼	Enable ▼
2	<input checked="" type="checkbox"/>	Shutdown Port ▼	Enable ▼
3	<input checked="" type="checkbox"/>	Shutdown Port ▼	Enable ▼
4	<input checked="" type="checkbox"/>	Shutdown Port ▼	Enable ▼
5	<input checked="" type="checkbox"/>	Shutdown Port ▼	Enable ▼
6	<input checked="" type="checkbox"/>	Shutdown Port ▼	Enable ▼
7	<input checked="" type="checkbox"/>	Shutdown Port ▼	Enable ▼
8	<input checked="" type="checkbox"/>	Shutdown Port ▼	Enable ▼

Save Reset

Object	Description
<b>General Settings</b>	
<b>Enable Loop Protection</b>	Controls whether loop protections is enabled (as a whole).
<b>Transmission Time</b>	The interval between each loop protection PDU sent on each port, valid values are 1 to 10 seconds.
<b>Shutdown Time</b>	The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800

	seconds (7 days). A value of zero will keep a port disabled (until next device restart).
<b>Port Configuration</b>	
<b>Port</b>	The switch port number of the port.
<b>Enable</b>	Controls whether loop protection is enabled on this switch port.
<b>Action</b>	Configures the action performed when a loop is detected on a port. Valid values are <b>Shutdown Port</b> , <b>Shutdown Port and Log</b> or <b>Log Only</b> .
<b>Tx Mode</b>	Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

<b>Buttons</b>	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## 3.0 Spanning Tree

### 3.0.1 Bridge Settings

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch

**DIGISOL™** **DG-IS4508HP**

▼ **Configuration**

- ▶ System
- ▶ Green Ethernet
- ▶ Ports
- ▶ DHCP
- ▶ Security
- ▶ Aggregation
- ▶ Loop Protection
- ▼ **Spanning Tree**
  - **Bridge Settings**
  - MSTI Mapping
  - MSTI Priorities
  - CIST Ports
  - MSTI Ports
- ▶ IPMC Profile
- MVR
- ▶ IPMC
- ▶ LLDP
- ▶ PoE
- MAC Table
- VLANs
- ▶ Private VLANs
- ▶ VCL
- ▶ Voice VLAN
- ▶ QoS

### STP Bridge Configuration

**Basic Settings**

Protocol Version	MSTP ▼
Bridge Priority	32768 ▼
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

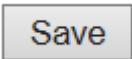
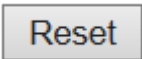
**Advanced Settings**

Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	

Save Reset

Object	Description
<b>Basic Settings</b>	
<b>Protocol Version</b>	The <a href="#">MSTP</a> / <a href="#">RSTP</a> / <a href="#">STP</a> protocol version setting. Valid values are <b>STP</b> , <b>RSTP</b> and <b>MSTP</b> .
<b>Bridge Priority</b>	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a <i>Bridge Identifier</i> .  For <b>MSTP</b> operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge

<b>Forward Delay</b>	The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.
<b>Max Age</b>	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds
<b>Maximum Hop Count</b>	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.
<b>Transmit Hold Count</b>	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.
<b>Advanced Settings</b>	
<b>Edge Port BPDU Filtering</b>	Control whether a port <i>explicitly</i> configured as <b>Edge</b> will transmit and receive BPDUs.
<b>Edge Port BPDU Guard</b>	Control whether a port <i>explicitly</i> configured as <b>Edge</b> will disable itself upon reception of a BPDU. The port will enter the <i>error-disabled</i> state, and will be removed from the active topology.
<b>Port Error Recovery</b>	Control whether a port in the <i>error-disabled</i> state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.
<b>Port Error Recovery Timeout</b>	The time to pass before a port in the <i>error-disabled</i> state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

### 3.0.2 MSTI Mapping

This page allows the user to inspect the current [STP](#) MSTI bridge instance priority configurations, and possibly change them as well.

**DIGISOL™** **DG-IS4508HP Industrial Ethernet**

**Configuration**

- System
- Green Ethernet
- Ports
- DHCP
- Security
- Aggregation
- Loop Protection
- Spanning Tree
  - Bridge Settings
  - MSTI Mapping
  - MSTI Priorities
  - CIST Ports
  - MSTI Ports
- IPMC Profile
  - MVR
  - IPMC
  - LLDP
  - PoE
  - MAC Table
  - VLANs
  - Private VLANs
  - VCL
  - Voice VLAN
  - QoS
  - Mirroring
  - GVRP
  - sFlow
  - RingV2
  - DDMI
- Monitor
- Diagnostics
- Maintenance
  - Restart Device
  - Factory Defaults

**MSTI Configuration**

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

**Configuration Identification**

Configuration Name: 00-17-7c-6a-bd-72

Configuration Revision: 0

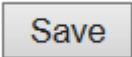
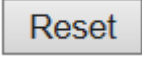
**MSTI Mapping**

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

Save Reset

Object	Description
<b>Configuration Identification</b>	
<b>Configuration Name</b>	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.
<b>Configuration Revision</b>	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.
<b>MSTI Mapping</b>	
<b>MSTI</b>	The bridge instance. The CIST is not available for explicit mapping, as it will receive

	the VLANs not explicitly mapped.
<b>VLANs Mapped</b>	The list of VLANs mapped to the MSTI. The VLANs can be given as a single ( <b>xx</b> , xx being between 1 and 4094) VLAN, or a range ( <b>xx-yy</b> ), each of which must be separated with comma and/or space. A VLAN can only be mapped to <i>one</i> MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Example: <b>2, 5, 20-40</b> .

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.



### 3.0.3 MSTI Priorities

This page allows the user to inspect the current [STP](#) MSTI bridge instance priority configurations, and possibly change them as well.

**DIGISOL™**

**Configuration**

- System
- Green Ethernet
- Ports
- DHCP
- Security
- Aggregation
- Loop Protection
- Spanning Tree
  - Bridge Settings
  - MSTI Mapping
  - MSTI Priorities
  - CIST Ports
  - MSTI Ports
- IPMC Profile
  - MVR
- IPMC
- LLDP
- PoE
- MAC Table
- VLANs
- Private VLANs
- VCI

**MSTI Configuration**

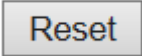
MSTI Priority Configuration

MSTI	Priority
*	<>
CIST	32768
MSTI1	32768
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768

Save Reset

Object	Description
<b>MSTI</b>	The bridge instance. The CIST is the <i>default</i> instance, which is always active.
<b>Priorities</b>	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a <i>Bridge Identifier</i> .

Buttons	
Save	Click to save changes.

	Click to undo any changes made locally and revert to previously saved values.
---	---

### 3.0.4 CIST Ports

This page allows the user to inspect the current [STP](#) CIST port configurations, and possibly change them as well.

This page contains settings for physical and [aggregated](#) ports.

**DIGISOL™** DG-IS4508HP Industrial Ethernet Switch

**STP CIST Port Configuration**

**CIST Aggregated Port Configuration**

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
-	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True

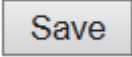
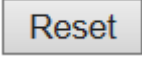
**CIST Normal Port Configuration**

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
*	<input checked="" type="checkbox"/>	<>	<>	<>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
3	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
4	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
5	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
6	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
7	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
8	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

Save Reset

Object	Description
<b>Port</b>	The switch port number of the logical STP port.
<b>STP Enabled</b>	Controls whether STP is enabled on this switch port.
<b>Path Cost</b>	Controls the path cost incurred by the port. The <b>Auto</b> setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the <b>Specific</b> setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.
<b>Priority</b>	Controls the port priority. This can be used to control priority of ports having identical

	port cost. (See above).
<b>operEdge (state flag)</b>	Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having <i>operEdge true</i> ) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.
<b>AdminEdge</b>	Controls whether the <i>operEdge</i> flag should start as set or cleared. (The initial <i>operEdge</i> state when a port is initialized).
<b>AutoEdge</b>	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows <i>operEdge</i> to be derived from whether BPDU's are received on the port or not.
<b>Restricted Role</b>	If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as <b>Root Guard</b> .
<b>Restricted TCN</b>	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.
<b>BPDU Guard</b>	<p>If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port <b>Edge</b> status does not effect this setting.</p> <p>A port entering error-disabled state due to this setting is subject to the bridge <a href="#">Port Error Recovery</a> setting as well.</p>
<b>Point-to-Point</b>	Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

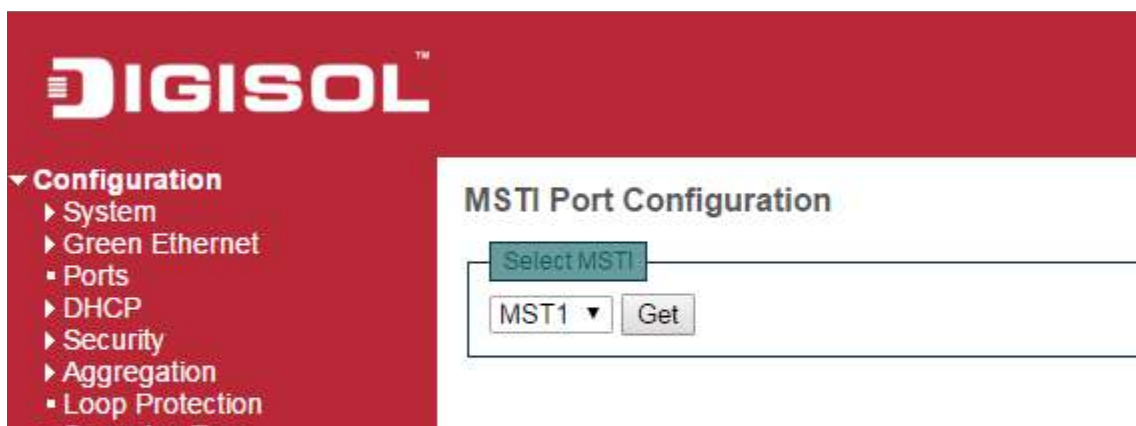
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.


### 3.0.5 MSTI Ports

This page allows the user to inspect the current [STP](#) MSTI port configurations, and possibly change them as well.

An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and [aggregated](#) ports.



Click  to retrieve settings for a specific MSTI, the page displayed as follow.

DIGISOL™

DG-IS4508H

▼ **Configuration**

- ▶ System
- ▶ Green Ethernet
- ▶ Ports
- ▶ DHCP
- ▶ Security
- ▶ Aggregation
- ▶ Loop Protection
- ▼ **Spanning Tree**
  - Bridge Settings
  - MSTI Mapping
  - MSTI Priorities
  - CIST Ports
  - MSTI Ports
- ▶ IPMC Profile
- MVR
- ▶ IPMC
- ▶ LLDP
- ▶ PoE
- MAC Table
- VLANs
- ▶ Private VLANs
- ▶ VCL
- ▶ Voice VLAN
- ▶ QoS
- Mirroring
- ▶ GVRP
- sFlow

### MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost	Priority
-	Auto ▼	128 ▼

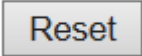
MSTI Normal Ports Configuration

Port	Path Cost	Priority
*	<> ▼	<> ▼
1	Auto ▼	128 ▼
2	Auto ▼	128 ▼
3	Auto ▼	128 ▼
4	Auto ▼	128 ▼
5	Auto ▼	128 ▼
6	Auto ▼	128 ▼
7	Auto ▼	128 ▼
8	Auto ▼	128 ▼

Save
Reset

Object	Description
<b>Port</b>	The switch port number of the corresponding STP CIST (and MSTI) port.
<b>Path Cost</b>	Controls the path cost incurred by the port. The <b>Auto</b> setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the <b>Specific</b> setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.
<b>Priority</b>	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

Buttons	
<div style="border: 1px solid #ccc; padding: 5px 15px; display: inline-block;">Get</div>	Click to retrieve settings for a specific MSTI.
<div style="border: 1px solid #ccc; padding: 5px 15px; display: inline-block;">Save</div>	Click to save changes.

	Click to undo any changes made locally and revert to previously saved values.
---	---



## 3.1 IPMC Profile



### 3.1.1 Profile Table


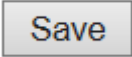
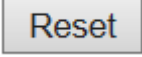
This page provides [IPMC Profile](#) related configurations.

The [IPMC](#) profile is used to deploy the access control on [IP](#) multicast streams. It is allowed to create at maximum 64 Profiles with at maximum 128 corresponding rules for each.



Object	Description
<b>Global Profile Mode</b>	Enable/Disable the Global IPMC Profile. System starts to do filtering based on profile settings only when the global profile mode is enabled.
<b>Delete</b>	Check to delete the entry. The designated entry will be deleted during the next save.
<b>Profile Name</b>	The name used for indexing the profile table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.
<b>Profile Description</b>	Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile.

	No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.
<b>Rule</b>	<p>When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons:</p> <p>: List the rules associated with the designated profile.</p> <p>: Adjust the rules associated with the designated profile.</p>

Buttons	
	Click to add new IPMC profile. Specify the name and configure the new entry. Click "Save".
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

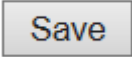
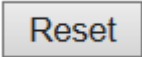

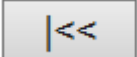

### 3.1.2 Address Entry

This page provides address range settings used in [IPMC profile](#).

The address entry is used to specify the address range that will be associated with [IPMC](#) Profile. It is allowed to create at maximum 128 address entries in the system.

Object	Description
<b>Delete</b>	Check to delete the entry. The designated entry will be deleted during the next save.
<b>Entry Name</b>	The name used for indexing the address entry table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.
<b>Start Address</b>	The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.
<b>End Address</b>	The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

Buttons	
<b>Add New Address (Range) Entry</b>	Click to add new address range. Specify the name and configure the addresses. Click "Save"

	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.
	Refreshes the displayed table starting from the input fields.
	Updates the table starting from the first entry in the IPMC Profile Address Configuration.
	Updates the table, starting with the entry after the last entry currently displayed.

## 3.2 MVR

This page provides [MVR](#) related configurations.

The MVR feature enables multicast traffic forwarding on the Multicast [VLANs](#).

In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an [IGMP/MLD](#) report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

It is allowed to create at maximum 4 MVR VLANs with corresponding channel profile for each Multicast VLAN.

The channel profile is defined by the [IPMC Profile](#) which provides the filtering conditions.

**DIGISOL™** **DG-IS4508HP Industrial Ethernet Switch**

**Configuration**

- System
- Green Ethernet
- Ports
- DHCP
- Security
- Aggregation
- Loop Protection
- Spanning Tree
- IPMC Profile
  - Profile Table
  - Address Entry
- MVR
- IPMC
- LLDP
- PoE
- MAC Table
- VLANs
- Private VLANs
- VCL
- Voice VLAN
- QoS
- Mirroring
- GVRP
- sFlow
- RingV2
- DDMI

**Monitor**

- System
- Green Ethernet
- Ports
- DHCP

**MVR Configurations**

MVR Mode: Disabled

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

Delete	MVR VID	MVR Name	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile
Add New MVR VLAN								


Immediate Leave Setting

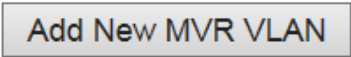
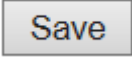
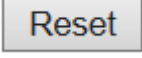
Port	Immediate Leave
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled

Save Reset

Object	Description
--------	-------------

<b>MVR Mode</b>	<p>Enable/Disable the Global MVR.</p> <p>The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping.</p> <p>It is suggested to enable Unregistered Flooding control when the MVR group table is full.</p>
<b>Delete</b>	Check to delete the entry. The designated entry will be deleted during the next save.
<b>MVR VID</b>	<p>Specify the Multicast <a href="#">VLAN ID</a>.</p> <p><b>Be Caution:</b> MVR source ports are not recommended to be overlapped with management VLAN ports.</p>
<b>MVR Name</b>	<p>MVR Name is an optional attribute to indicate the name of the specific MVR VLAN.</p> <p>Maximum length of the MVR VLAN Name string is 16. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.</p>
<b>IGMP Address</b>	<p>Define the IPv4 address as source address used in IP header for <a href="#">IGMP</a> control frames.</p> <p>The default IGMP address is not set (0.0.0.0).</p> <p>When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.</p> <p>When the IPv4 management address is not set, system uses the first available IPv4 management address.</p> <p>Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.</p>
<b>Mode</b>	Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.
<b>Tagging</b>	Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.
<b>Priority</b>	Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.
<b>LLQI</b>	Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.
<b>Interface Channel Profile</b>	When the MVR VLAN is created, select the <a href="#">IPMC Profile</a> as the channel filtering condition for the specific MVR VLAN. Summary about the Interface Channel Profiling (of the MVR VLAN) will be shown by clicking the view button. Profile selected for

	designated interface channel is not allowed to have overlapped permit group address.
<b>Profile Management Button</b>	You can inspect the rules of the designated profile by using the following button:  : List the rules associated with the designated profile.
<b>Port</b>	The logical port for the settings.
<b>Port Role</b>	<p>Configure an MVR port of the designated MVR VLAN as one of the following roles.</p> <p><b>Inactive:</b> The designated port does not participate MVR operations.</p> <p><b>Source:</b> Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.</p> <p><b>Receiver:</b> Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.</p> <p><b>Be Caution:</b> MVR source ports are not recommended to be overlapped with management VLAN ports.</p> <p>Select the port role by clicking the Role symbol to switch the setting.</p> <p>I indicates Inactive; S indicates Source; R indicates Receiver</p> <p>The default Role is Inactive.</p>
<b>Immediate Leave</b>	Enable the <a href="#">fast leave</a> on the port.

Buttons	
	Click to add new MVR VLAN. Specify the VID and configure the new entry. Click "Save".
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## 3.3 IPMC

### 3.3.1 IGMP Snooping

#### Basic Configuration

This page provides [IGMP](#) Snooping related configuration.

**DIGISOL™** **DG-IS4508HP**

**Configuration**

- System
- Green Ethernet
- Ports
- DHCP
- Security
- Aggregation
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC**
  - IGMP Snooping**
    - Basic Configuration
    - VLAN Configuration
    - Port Filtering Profile
  - MLD Snooping
- LLDP
- PoE
- MAC Table
- VLANs
- Private VLANs
- VCL
- Voice VLAN
- QoS
- Mirroring
- GVRP
- sFlow
- RingV2

**IGMP Snooping Configuration**

**Global Configuration**

Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv4 Flooding Enabled	<input checked="" type="checkbox"/>
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	<input type="checkbox"/>
Proxy Enabled	<input type="checkbox"/>

**Port Related Configuration**

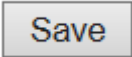
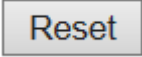
Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	<> ▼
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼

Save Reset

Object	Description
<b>Snooping Enabled</b>	Enable the Global IGMP Snooping.
<b>Unregistered IPMCv4 Flooding Enabled</b>	<p>Enable unregistered IPMCv4 traffic flooding.</p> <p>The flooding control takes effect only when IGMP Snooping is enabled.</p> <p>When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always</p>



	active in spite of this setting.
<b>IGMP SSM Range</b>	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
<b>Leave Proxy Enabled</b>	Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
<b>Proxy Enabled</b>	Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
<b>Router Port</b>	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or <a href="#">IGMP querier</a> .  If an <a href="#">aggregation</a> member port is selected as a router port, the whole aggregation will act as a router port.
<b>Fast Leave</b>	Enable the fast leave on the port.
<b>Throttling</b>	Enable to limit the number of multicast groups to which a switch port can belong.

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

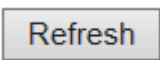
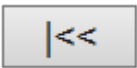

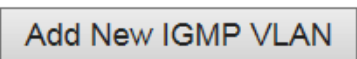
## VLAN Configuration

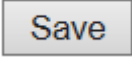
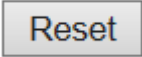
Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest [VLAN ID](#) found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table.

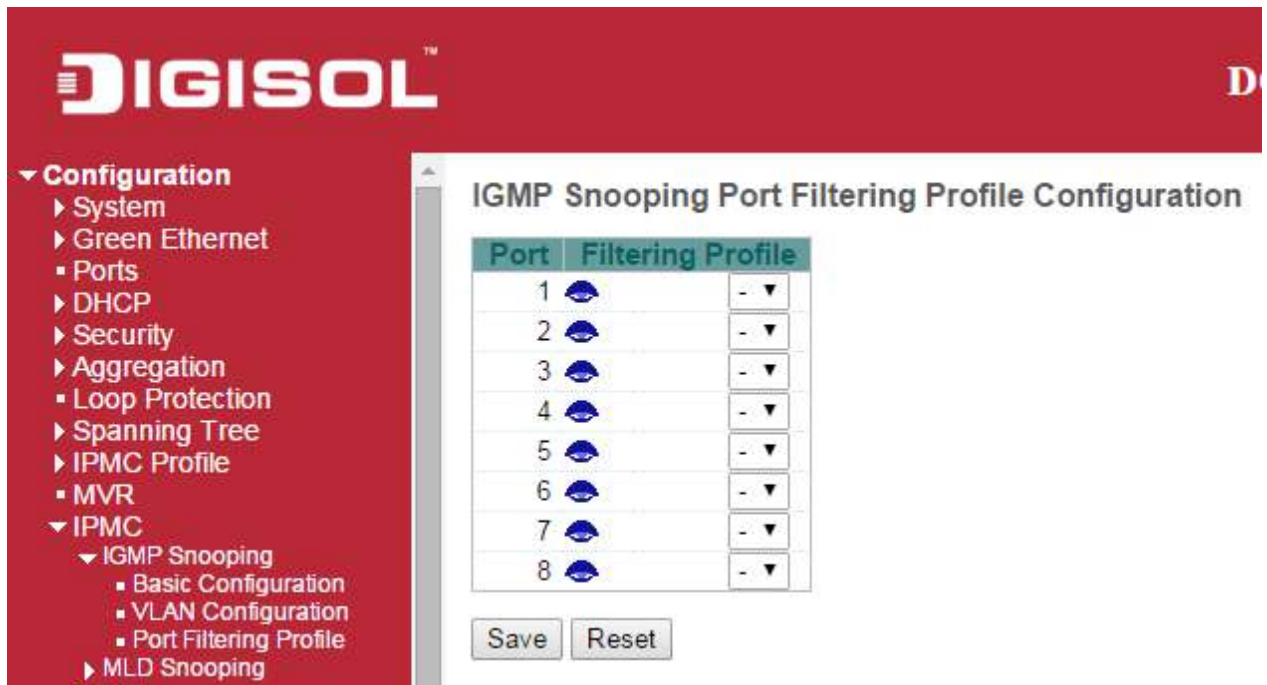
Object	Description
<b>Delete</b>	Check to delete the entry. The designated entry will be deleted during the next save.
<b>VLAN ID</b>	The VLAN ID of the entry.
<b>IGMP Snooping Enabled</b>	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
<b>Querier Election</b>	Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
<b>Querier Address</b>	<p>Define the IPv4 address as source address used in IP header for IGMP <a href="#">Querier election</a>.</p> <p>When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.</p> <p>When the IPv4 management address is not set, system uses the first available IPv4 management address.</p> <p>Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.</p>
<b>Compatibility</b>	<p>Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network.</p> <p>The allowed selection is <b>IGMP-Auto</b>, <b>Forced IGMPv1</b>, <b>Forced IGMPv2</b>, <b>Forced</b></p>


	<b>IGMPv3</b> , default compatibility value is IGMP-Auto.
<b>PRI</b>	<p>Priority of Interface.</p> <p>It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.</p> <p>The allowed range is <b>0</b> (best effort) to <b>7</b> (highest), default interface priority value is 0.</p>
<b>RV</b>	<p>Robustness Variable.</p> <p>The Robustness Variable allows tuning for the expected packet loss on a network.</p> <p>The allowed range is <b>1</b> to <b>255</b>, default robustness variable value is 2.</p>
<b>QI</b>	<p>Query Interval.</p> <p>The Query Interval is the interval between General Queries sent by the Querier.</p> <p>The allowed range is <b>1</b> to <b>31744</b> seconds, default query interval is 125 seconds.</p>
<b>QRI</b>	<p>Query Response Interval.</p> <p>The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.</p> <p>The allowed range is <b>0</b> to <b>31744</b> in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).</p>
<b>LLQI(LMQI for IGMP)</b>	<p>Last Member Query Interval.</p> <p>The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count.</p> <p>The allowed range is <b>0</b> to <b>31744</b> in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).</p>
<b>URI</b>	<p>Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group.</p> <p>The allowed range is <b>0</b> to <b>31744</b> seconds, default unsolicited report interval is 1 second.</p>

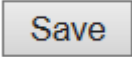
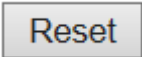
Buttons	
	Refreshes the displayed table starting from the "VLAN" input fields.
	Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.
	Updates the table, starting with the entry after the last entry currently displayed.
	Click to add new IGMP VLAN. Specify the VID and configure the new entry. Click "Save". The specific IGMP VLAN starts working after the

	corresponding static VLAN is also created.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## Port Filtering Profile



Object	Description
<b>Port</b>	The logical port for the settings.
<b>Filtering Profile</b>	Select the <a href="#">IPMC Profile</a> as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.
<b>Profile Management Button</b>	You can inspect the rules of the designated profile by using the following button:  : List the rules associated with the designated profile.

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.



### 3.3.2 MLD Snooping

#### Basic Configuration

This page provides [MLD](#) Snooping related configuration.

**DIGISOL™** DG-IS4508HP Industrial Ethernet

▼ Configuration

- System
- Green Ethernet
- Ports
- DHCP
- Security
- Aggregation
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- ▼ IPMC
  - ▼ IGMP Snooping
    - Basic Configuration
    - VLAN Configuration
    - Port Filtering Profile
  - ▼ MLD Snooping
    - Basic Configuration
    - VLAN Configuration
    - Port Filtering Profile
- LLDP
- PoE
- MAC Table
- VLANs
- Private VLANs
- VCL
- Voice VLAN
- QoS
- Mirroring
- GVRP

#### MLD Snooping Configuration

##### Global Configuration

Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv6 Flooding Enabled	<input checked="" type="checkbox"/>
MLD SSM Range	ff3e:: / 96
Leave Proxy Enabled	<input type="checkbox"/>
Proxy Enabled	<input type="checkbox"/>

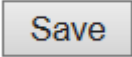
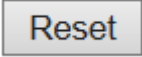
##### Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

Save Reset

Object	Description
<b>Snooping Enable</b>	Enable the Global MLD Snooping.
<b>Unregistered IPMCv6 Flooding Enable</b>	Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.
<b>MLD SSM Range</b>	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
<b>Leave Proxy Enable</b>	Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
<b>Proxy Enable</b>	Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

<b>Router Port</b>	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or <a href="#">MLD querier</a> . If an <a href="#">aggregation</a> member port is selected as a router port, the whole aggregation will act as a router port.
<b>Fast Leave</b>	Enable the fast leave on the port.
<b>Throttling</b>	Enable to limit the number of multicast groups to which a switch port can belong.

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.



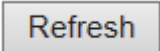
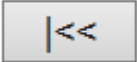
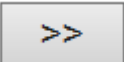
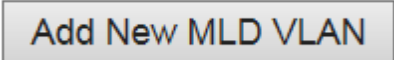
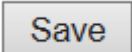
## VLAN Configuration

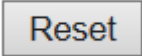
Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest [VLAN ID](#) found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table.

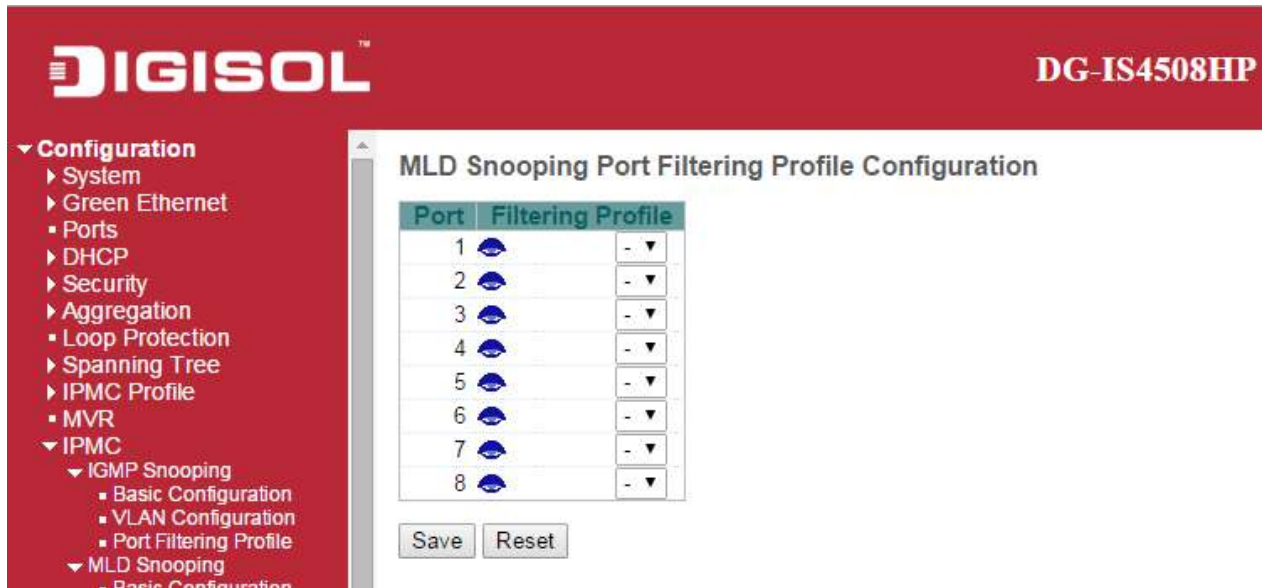
Object	Description
<b>Delete</b>	Check to delete the entry. The designated entry will be deleted during the next save.
<b>VLAN ID</b>	The VLAN ID of the entry.
<b>MLD Snooping Enabled</b>	Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.
<b>Querier Election</b>	Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.
<b>Compatibility</b>	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is <b>MLD-Auto</b> , <b>Forced MLDv1</b> , <b>Forced MLDv2</b> , default compatibility value is MLD-Auto.
<b>PRI</b>	Priority of Interface. It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is <b>0</b> (best effort) to <b>7</b> (highest), default interface priority value is 0.
<b>RV</b>	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a link. The allowed range is <b>1</b> to <b>255</b> , default robustness variable value is 2.

<b>QI</b>	<p>Query Interval.</p> <p>The Query Interval is the interval between General Queries sent by the Querier.</p> <p>The allowed range is <b>1</b> to <b>31744</b> seconds, default query interval is 125 seconds.</p>
<b>QRI</b>	<p>Query Response Interval.</p> <p>The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.</p> <p>The allowed range is <b>0</b> to <b>31744</b> in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).</p>
<b>LLQI</b>	<p>Last Listener Query Interval.</p> <p>The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages.</p> <p>The allowed range is <b>0</b> to <b>31744</b> in tenths of seconds, default last listener query interval is 10 in tenths of seconds (1 second).</p>
<b>URI</b>	<p>Unsolicited Report Interval.</p> <p>The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address.</p> <p>The allowed range is <b>0</b> to <b>31744</b> seconds, default unsolicited report interval is 1 second.</p>

Buttons	
	Refreshes the displayed table starting from the "VLAN" input fields.
	Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.
	Updates the table, starting with the entry after the last entry currently displayed.
	Click to add new MLD VLAN. Specify the VID and configure the new entry. Click "Save". The specific MLD VLAN starts working after the corresponding static VLAN is also created.
	Click to save changes.

	Click to undo any changes made locally and revert to previously saved values.
---	---

## Port Filtering Profile



Object	Description
<b>Port</b>	The logical port for the settings.
<b>Filtering Profile</b>	Select the <a href="#">IPMC Profile</a> as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.
<b>Profile Management Button</b>	You can inspect the rules of the designated profile by using the following button: : List the rules associated with the designated profile.

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## 3.4 LLDP

### 3.4.1 LLDP

This page allows the user to inspect and configure the current [LLDP](#) port settings.

**DIGISOL™** DG-IS4508HP Industrial Ethernet Switch

**Configuration**

- System
- Green Ethernet
- Ports
- DHCP
- Security
- Aggregation
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
  - LLDP
  - LLDP-MED
- PoE
- MAC Table
- VLANs
- Private VLANs
- VCL
- Voice VLAN
- QoS
- Mirroring
- GVRP
- sFlow
- RingV2
- DDMI

**Monitor**

- System
- Green Ethernet
- Ports

**LLDP Configuration**

**LLDP Parameters**

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

**LLDP Port Configuration**

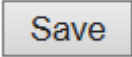
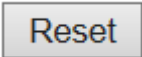
Port	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Save Reset

Object	Description
<b>LLDP Parameters</b>	
<b>Tx Interval</b>	The switch periodically transmits <a href="#">LLDP</a> frames to its neighbors for having the network discovery information up-to-date. The interval between each <a href="#">LLDP</a> frame is determined by the <b>Tx Interval</b> value. Valid values are restricted to 5 - 32768 seconds.
<b>Tx Hold</b>	Each <a href="#">LLDP</a> frame contains information about how long the information in the <a href="#">LLDP</a> frame shall be considered valid. The <a href="#">LLDP</a> information valid period is set to <b>Tx Hold</b> multiplied by <b>Tx Interval</b> seconds. Valid values are restricted to 2 - 10 times.
<b>Tx Delay</b>	If some configuration is changed (e.g. the IP address) a new <a href="#">LLDP</a> frame is transmitted, but the time between the <a href="#">LLDP</a> frames will always be at least the value of <b>Tx Delay</b> seconds. <b>Tx Delay</b> cannot be larger than 1/4 of the <b>Tx Interval</b> value.

	Valid values are restricted to 1 - 8192 seconds.
<b>Tx Reinit</b>	When a port is disabled, <a href="#">LLDP</a> is disabled or the switch is rebooted, an <a href="#">LLDP</a> shutdown frame is transmitted to the neighboring units, signalling that the <a href="#">LLDP</a> information isn't valid anymore. <b>Tx Reinit</b> controls the amount of seconds between the shutdown frame and a new <a href="#">LLDP</a> initialization. Valid values are restricted to 1 - 10 seconds.
<b>LLDP Port Parameters</b>	
<b>Port</b>	The switch port number of the logical <a href="#">LLDP</a> port.
<b>Mode</b>	<p>Select <a href="#">LLDP</a> mode.</p> <p><b>Rx only</b> The switch will not send out <a href="#">LLDP</a> information, but <a href="#">LLDP</a> information from neighbor units is analyzed.</p> <p><b>Tx only</b> The switch will drop <a href="#">LLDP</a> information received from neighbors, but will send out <a href="#">LLDP</a> information.</p> <p><b>Disabled</b> The switch will not send out <a href="#">LLDP</a> information, and will drop <a href="#">LLDP</a> information received from neighbors.</p> <p><b>Enabled</b> The switch will send out <a href="#">LLDP</a> information, and will analyze <a href="#">LLDP</a> information received from neighbors.</p>
<b>CDP Aware</b>	<p>Select <a href="#">CDP</a> awareness.</p> <p>The <a href="#">CDP</a> operation is restricted to decoding incoming <a href="#">CDP</a> frames (The switch doesn't transmit <a href="#">CDP</a> frames). <a href="#">CDP</a> frames are only decoded if <a href="#">LLDP</a> on the port is enabled.</p> <p>Only <a href="#">CDP</a> TLVs that can be mapped to a corresponding field in the <a href="#">LLDP</a> neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). <a href="#">CDP</a> TLVs are mapped onto <a href="#">LLDP</a> neighbors' table as shown below.</p> <p><a href="#">CDP</a> TLV "Device ID" is mapped to the <a href="#">LLDP</a> "Chassis ID" field.</p> <p><a href="#">CDP</a> TLV "Address" is mapped to the <a href="#">LLDP</a> "Management Address" field. The <a href="#">CDP</a> address TLV can contain multiple addresses, but only the first address is shown in the <a href="#">LLDP</a> neighbors table.</p> <p><a href="#">CDP</a> TLV "Port ID" is mapped to the <a href="#">LLDP</a> "Port ID" field.</p> <p><a href="#">CDP</a> TLV "Version and Platform" is mapped to the <a href="#">LLDP</a> "System Description" field.</p> <p>Both the <a href="#">CDP</a> and <a href="#">LLDP</a> support "system capabilities", but the <a href="#">CDP</a> capabilities cover capabilities that are not part of the <a href="#">LLDP</a>. These capabilities are shown as "others" in the <a href="#">LLDP</a> neighbors' table.</p> <p>If all ports have <a href="#">CDP</a> awareness disabled the switch forwards <a href="#">CDP</a> frames received from neighbor devices. If at least one port has <a href="#">CDP</a> awareness enabled all <a href="#">CDP</a></p>

	frames are terminated by the switch.  Note: When <a href="#">CDP</a> awareness on a port is disabled the <a href="#">CDP</a> information isn't removed immediately, but gets removed when the hold time is exceeded.
<b>Port Descr</b>	<a href="#">Optional TLV</a> : When checked the "port description" is included in <a href="#">LLDP</a> information transmitted.
<b>Sys Name</b>	<a href="#">Optional TLV</a> : When checked the "system name" is included in <a href="#">LLDP</a> information transmitted.
<b>Sys Descr</b>	<a href="#">Optional TLV</a> : When checked the "system description" is included in <a href="#">LLDP</a> information transmitted.
<b>Sys Capa</b>	<a href="#">Optional TLV</a> : When checked the "system capability" is included in <a href="#">LLDP</a> information transmitted.
<b>Mgmt Addr</b>	<a href="#">Optional TLV</a> : When checked the "management address" is included in <a href="#">LLDP</a> information transmitted.

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

### 3.4.2 LLDP-MED

This page allows you to configure the [LLDP-MED](#). This function applies to VoIP devices which support LLDP-MED.


Object	Description
<b>Fast start repeat count</b>	
<b>Fast start repeat count</b>	<p>Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPDU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.</p> <p>With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors.</p> <p>Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to</p>



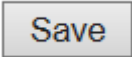
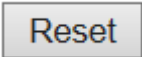
	<p>increase the possibility of the neighbors receiving the LLDP frame. With <b>Fast start repeat count</b> it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.</p> <p>It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.</p>
<b>Coordinates Location</b>	
<b>Latitude</b>	<p><b>Latitude</b> SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits.</p> <p>It is possible to specify the direction to either <b>North</b> of the equator or <b>South</b> of the equator.</p>
<b>Longitude</b>	<p><b>Longitude</b> SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits.</p> <p>It is possible to specify the direction to either <b>East</b> of the prime meridian or <b>West</b> of the prime meridian.</p>
<b>Altitude</b>	<p><b>Altitude</b> SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits.</p> <p>It is possible to select between two altitude types (floors or meters).</p> <p><b>Meters:</b> Representing meters of Altitude defined by the vertical datum specified.</p> <p><b>Floors:</b> Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.</p>
<b>Map Datum</b>	<p>The <b>Map Datum</b> is used for the coordinates given in these options:</p> <p><b>WGS84:</b> (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.</p> <p><b>NAD83/NAVD88:</b> North American Datum 1983, CRS Code 4269, Prime Meridian</p>

	<p>Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).</p> <p><b>NAD83/MLLW:</b> North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.</p>
<b>Civic Address Location</b>	
<b>Country code</b>	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
<b>State</b>	National subdivisions (state, canton, region, province, prefecture).
<b>County</b>	County, parish, gun (Japan), district.
<b>City</b>	City, township, shi (Japan) - Example: Copenhagen.
<b>City district</b>	City division, borough, city district, ward, chou (Japan).
<b>Block (Neighborhood)</b>	Neighborhood, block.
<b>Street</b>	Street - Example: Poppelvej.
<b>Leading street direction</b>	Leading street direction - Example: N.
<b>Trailing street suffix</b>	Trailing street suffix - Example: SW.
<b>Street suffix</b>	Street suffix - Example: Ave, Platz.
<b>House no.</b>	House number - Example: 21.
<b>House no. suffix</b>	House number suffix - Example: A, 1/2.
<b>Landmark</b>	Landmark or vanity address - Example: Columbia University.
<b>Additional location info</b>	Additional location info - Example: South Wing.
<b>Name</b>	Name (residence and office occupant) - Example: Flemming Jahn.
<b>Zip code</b>	Postal/zip code - Example: 2791.
<b>Building</b>	Building (structure) - Example: Low Library.
<b>Apartment</b>	Unit (Apartment, suite) - Example: Apt 42.
<b>Floor</b>	Floor - Example: 4.
<b>Room no.</b>	Room number - Example: 450F.
<b>Place type</b>	Place type - Example: Office.
<b>Postal community name</b>	Postal community name - Example: Leonia.
<b>P.O. Box</b>	Post office box (P.O. BOX) - Example: 12345.
<b>Additional code</b>	Additional code - Example: 1320300003.
<b>Emergency Call Service</b>	
<b>Emergency Call Service</b>	<b>Emergency Call Service</b> ELIN identifier data format is defined to carry the ELIN

	identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.
<b>Policies</b>	
<b>Delete</b>	Check to delete the policy. It will be deleted during the next save.
<b>Policy ID</b>	ID for the policy. This is auto generated and shall be used when selecting the policies that shall be mapped to the specific ports.
<b>Application Type</b>	<p>Intended use of the application types:</p> <ol style="list-style-type: none"> <li>1. <b>Voice</b> - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.</li> <li>2. <b>Voice Signalling</b> (conditional) - for use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the <b>Voice</b> application policy.</li> <li>3. <b>Guest Voice</b> - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.</li> <li>4. <b>Guest Voice Signalling</b> (conditional) - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the <b>Guest Voice</b> application policy.</li> <li>5. <b>Softphone Voice</b> - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.</li> <li>6. <b>Video Conferencing</b> - for use by dedicated Video Conferencing equipment and</li> </ol>

	<p>other similar appliances supporting real-time interactive video/audio services.</p> <p>7. <b>Streaming Video</b> - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.</p> <p>8. <b>Video Signalling</b> (conditional) - for use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the <b>Video Conferencing</b> application policy.</p>
<b>Tag</b>	<p><b>Tag</b> indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN.</p> <p><b>Untagged</b> indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.</p> <p><b>Tagged</b> indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.</p>
<b>VLAN ID</b>	VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.
<b>L2 Priority</b>	<p><b>L2 Priority</b> is the Layer 2 priority to be used for the specified application type. <b>L2 Priority</b> may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.</p>
<b>DSCP</b>	<p><b>DSCP</b> value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. <b>DSCP</b> may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.</p>
<b>Adding a new policy</b>	<p>Click  to add a new policy. Specify the <b>Application type</b>, <b>Tag</b>, <b>VLAN ID</b>, <b>L2 Priority</b> and <b>DSCP</b> for the new policy. Click "Save".</p>

	The number of policies supported is 32
<b>Port Policies Configuration</b>	
<b>Port</b>	The port number to which the configuration applies.
<b>Policy Id</b>	The set of policies that shall apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

### 3.5 PoE

This page allows the user to inspect and configure the current [PoE](#) port settings.

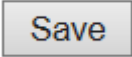
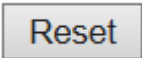
The screenshot shows the DIGISOL DG-IS4508HP Industrial switch configuration interface. The left sidebar contains a navigation menu with the following items: Configuration, System, Green Ethernet, Ports, DHCP, Security, Aggregation, Loop Protection, Spanning Tree, IPMC Profile, MVR, IPMC, LLDP, LLDP, LLDP-MED, PoE, PoE, Power Scheduler, Power Reset, MAC Table, VLANs, Private VLANs, VCL, Voice VLAN, and QoS. The main content area is titled "Power Over Ethernet Configuration". It includes three sections: "Reserved Power determined by" with radio buttons for Class (selected), Allocation, and LLDP-MED; "Power Management Mode" with radio buttons for Actual Consumption and Reserved Power (selected); and "PoE Power Supply Configuration" with a "Primary Power Supply [W]" field set to 120. Below this is the "PoE Port Configuration" table, which has columns for Port, Mode, Operation, Priority, and Maximum Power [W]. The table shows four ports, all with Mode set to "Disable", Operation set to "802.3af", Priority set to "Low", and Maximum Power set to "15.4". At the bottom of the table are "Save" and "Reset" buttons.

Object	Description
<b>Reserved Power determined by</b>	
<b>Allocated mode</b>	In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields.
<b>Class mode</b>	In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts. In this mode the Maximum Power fields have no effect.
<b>LLDP-MED mode</b>	This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode. In this mode the Maximum Power fields have no effect.
<b>Power Management Mode</b>	
<b>Actual Consumption</b>	In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are

	shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down.
<b>Reserved Power</b>	In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply.
<b>Power Supply Configuration</b>	
<b>Power Source</b>	For being able to determine the amount of power the PD may use, it must be defined what amount of power a power source can deliver. Valid values are in the range 0 to 240 Watts.
<b>Port Configuration</b>	
<b>Port</b>	This is the logical port number for this row. Ports that are not PoE-capable are grayed out and thus impossible to configure PoE for.
<b>PoE Mode</b>	
<b>Disable</b>	PoE disabled for the port.
<b>Enable</b>	Enables PoE for the port.
<b>Schedule</b>	Enables PoE for the port by scheduling.
<b>Operation Mode</b>	
<b>802.3af</b>	Sets PoE protocol to IEEE 802.3af.
<b>802.3at</b>	Sets PoE protocol to IEEE 802.3at.
<b>4Pairs</b>	
<b>Enable</b>	Enable 4Pairs to support 60W. The option is only available when following rules are applied. - High power model supports. - Only port1 or port2 supports - Current operation mode is 802.3at.
<b>Disable</b>	Disable 4Pairs to limit 30W of power.
<b>Priority</b>	
The priority is used in the case where the remote devices require more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.	
<b>Low</b>	The lowest priority
<b>High</b>	The medium priority
<b>Critical</b>	The highest priority
<b>Maximum Power</b>	
The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be	

delivered to a remote device.

For port support 4Pairs mode, the maximum allowed value is 60 W; others are 30 W.

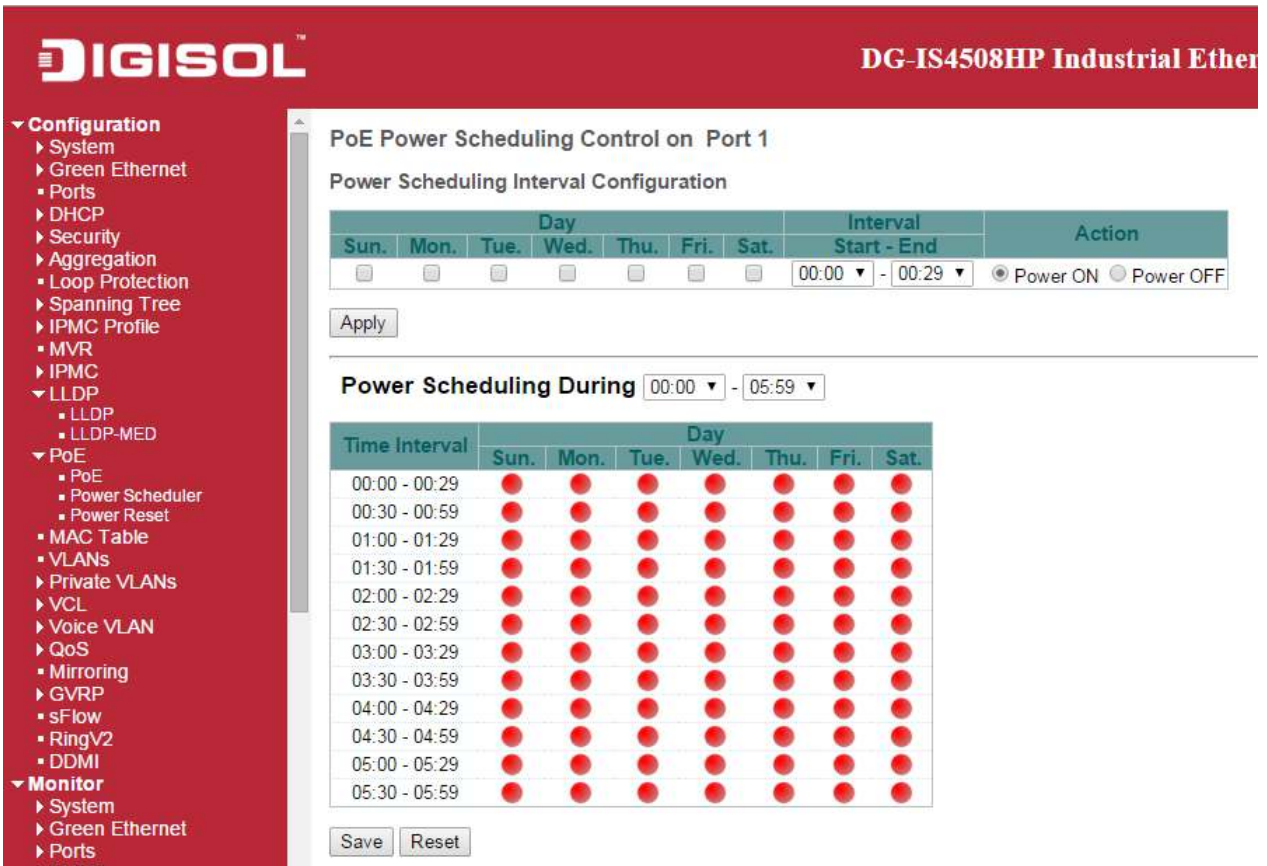
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

### 3.5.1 PoE Scheduler

This page provides power scheduling configurations.

The entry is used to control the power alive interval on PoE port.

It is allowed to set the specific interval to schedule power on/off in one week.



**DIGISOL™** DG-IS4508HP Industrial Ethernet

**Configuration**

- System
- Green Ethernet
- Ports
- DHCP
- Security
- Aggregation
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
  - LLDP
  - LLDP-MED
- PoE**
  - PoE
  - Power Scheduler
  - Power Reset
- MAC Table
- VLANs
- Private VLANs
- VCL
- Voice VLAN
- QoS
- Mirroring
- GVRP
- sFlow
- RingV2
- DDMI

**Monitor**

- System
- Green Ethernet
- Ports
- DHCP

**PoE Power Scheduling Control on Port 1**

Power Scheduling Interval Configuration

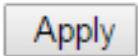
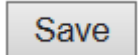

Day							Interval	Action
Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.	Start - End	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	00:00 - 00:29	<input checked="" type="radio"/> Power ON <input type="radio"/> Power OFF

Power Scheduling During 00:00 - 05:59

Time Interval	Day						
	Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.
00:00 - 00:29	●	●	●	●	●	●	●
00:30 - 00:59	●	●	●	●	●	●	●
01:00 - 01:29	●	●	●	●	●	●	●
01:30 - 01:59	●	●	●	●	●	●	●
02:00 - 02:29	●	●	●	●	●	●	●
02:30 - 02:59	●	●	●	●	●	●	●
03:00 - 03:29	●	●	●	●	●	●	●
03:30 - 03:59	●	●	●	●	●	●	●
04:00 - 04:29	●	●	●	●	●	●	●
04:30 - 04:59	●	●	●	●	●	●	●
05:00 - 05:29	●	●	●	●	●	●	●
05:30 - 05:59	●	●	●	●	●	●	●



Object	Description
<b>Power Scheduling Interval Configuration</b>	
<b>Day</b>	Checkmarks indicate which day are members of the set.
<b>Interval</b>	Start - Select the start hour and minute. End - Select the end hour and minute.
<b>Action</b>	Power On - Select the radio button to apply power on during the interval. Power Off - Select the radio button to apply power off during the interval.
<b>Power Scheduling During</b>	
<b>Time Interval</b>	There are 48 time interval one day. Each interval have 30 minutes.
<b>Day</b>	The current scheduling state is displayed graphically during the week. Green indicates the power is on and red that it is off. Directly changes checkmarks to indicate which day are members of the time interval. Check or uncheck as needed to modify the scheduling table.

Buttons	
	Click to apply the power scheduling interval.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

### 3.5.2 Power Reset

This page provides power reset entry configurations.

The entry is used to control the power reset time on PoE port.

It is allowed to create at maximum 5 entries for each PoE port.




Object	Description
<b>Delete</b>	Check to delete the entry. The designated entry will be deleted during the next save.
<b>Day</b>	Checkmarks indicate which day are members of the entry. Check or uncheck as needed to modify the entry.
<b>Time (hh:mm)</b>	hh - Select the hour. mm - Select the minute.

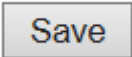
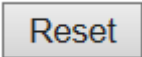
Buttons	
	Click to add new reset entry
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

### 3.5.3 MAC Table

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic [MAC Table](#) and configure the static MAC table here.

Object	Description
<b>Aging Configuration</b>	
<b>Disable Automatic Aging</b>	Disable the automatic aging of dynamic entries by ticking the item. <input type="checkbox"/>
<b>Aging Time</b>	Enter a value in seconds. The allowed range is 10 to 1000000 seconds.
<b>MAC Table Learning</b>	
<b>Auto</b>	Learning is done automatically as soon as a frame with unknown SMAC is received.
<b>Disable</b>	No learning is done.
<b>Secure</b>	Only static MAC entries are learned, all other frames are dropped. <b>Note:</b> Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is

	lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.
<b>Static MAC Table Learning</b>	
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>VLAN ID</b>	The VLAN ID of the entry.
<b>MAC Address</b>	The MAC address of the entry.
<b>Port Members</b>	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
<b>Adding a New Static Entry</b>	Click  to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

<b>Buttons</b>	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

### 3.5.4 VLANs

This page allows for controlling [VLAN](#) configuration on the switch.

The page is divided into a global section and a per-port configuration section.

Object	Description
<b>Global VLAN Configuration</b>	
<b>Allowed Access VLANs</b>	This field shows the allowed Access VLANs, i.e. it only affects ports configured as <a href="#">Access ports</a> . Ports in other modes are members of all VLANs specified in the <a href="#">Allowed VLANs</a> field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: <b>1, 10-13, 200, 300</b> . Spaces are allowed in between the delimiters.
<b>Ethertype for Custom S-ports</b>	This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose <a href="#">Port Type</a> is set to S-Custom-Port.
<b>Port VLAN Configuration</b>	
<b>Port</b>	This is the logical port number of this row.
<b>Mode</b>	The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below.  Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question.  Grayed out fields show the value that the port will get when the mode is applied.  <b>Access:</b>

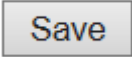
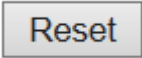
	<p>Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:</p> <ul style="list-style-type: none"> <li>• Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1</li> <li>• Accepts untagged and C-tagged frames</li> <li>• Discards all frames that are not classified to the Access VLAN</li> <li>• On egress all frames classified to the Access VLAN are transmitted untagged. Other (dynamically added VLANs) are transmitted tagged</li> </ul> <p><b><u>Trunk:</u></b></p> <p>Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:</p> <ul style="list-style-type: none"> <li>• By default, a trunk port is member of all VLANs (1-4095)</li> <li>• The VLANs that a trunk port is member of may be limited by the use of <a href="#">Allowed VLANs</a></li> <li>• Frames classified to a VLAN that the port is not a member of are discarded</li> <li>• By default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress</li> <li>• Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress</li> </ul> <p><b><u>Hybrid:</u></b></p> <p>Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:</p> <ul style="list-style-type: none"> <li>• Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware</li> <li>• Ingress filtering can be controlled</li> <li>• Ingress acceptance of frames and configuration of egress tagging can be configured independently</li> </ul>
--	--

<b>Port VLAN</b>	<p>Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095, default being 1.</p> <p>On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).</p> <p>On egress, frames classified to the Port VLAN do not get tagged if <a href="#">Egress Tagging</a> configuration is set to untag Port VLAN.</p> <p>The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.</p>
<b>Port Type</b>	<p>Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.</p> <p><b><u>Unaware:</u></b></p> <p>On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.</p> <p><b><u>C-Port:</u></b></p> <p>On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag.</p> <p><b><u>S-Port:</u></b></p> <p>On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.</p> <p><b><u>S-Custom-Port:</u></b></p> <p>On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the <a href="#">Ethertype configured for Custom-S ports</a> get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.</p>
<b>Ingress Filtering</b>	<p>Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.</p> <p>If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.</p> <p>If ingress filtering is disabled, frames classified to a VLAN that the port is not a</p>

	<p>member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.</p>
<b>Ingress Acceptance</b>	<p>Hybrid ports allow for changing the type of frames that are accepted on ingress.</p> <p><b><u>Tagged and Untagged</u></b></p> <p>Both tagged and untagged frames are accepted.</p> <p><b><u>Tagged Only</u></b></p> <p>Only tagged frames are accepted on ingress. Untagged frames are discarded.</p> <p><b><u>Untagged Only</u></b></p> <p>Only untagged frames are accepted on ingress. Tagged frames are discarded.</p>
<b>Egress Tagging</b>	<p>Ports in Trunk and Hybrid mode may control the tagging of frames on egress.</p> <p><b><u>Untag Port VLAN</u></b></p> <p>Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.</p> <p><b><u>Tag All</u></b></p> <p>All frames, whether classified to the Port VLAN or not, are transmitted with a tag.</p> <p><b><u>Untag All</u></b></p> <p>All frames, whether classified to the Port VLAN or not, are transmitted without a tag.</p> <p>This option is only available for ports in Hybrid mode.</p>
<b>Allowed VLANs</b>	<p>Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN.</p> <p>The field's syntax is identical to the syntax used in the <a href="#">Enabled VLANs</a> field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to 1-4095.</p> <p>The field may be left empty, which means that the port will not become member of any VLANs.</p>
<b>Forbidden VLANs</b>	<p>A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs.</p> <p>The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the <a href="#">Enabled VLANs</a> field.</p> <p>By default, the field is left blank, which means that the port may become a member of all possible VLANs.</p>

**Buttons**



	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## 3.6 Private VLANs

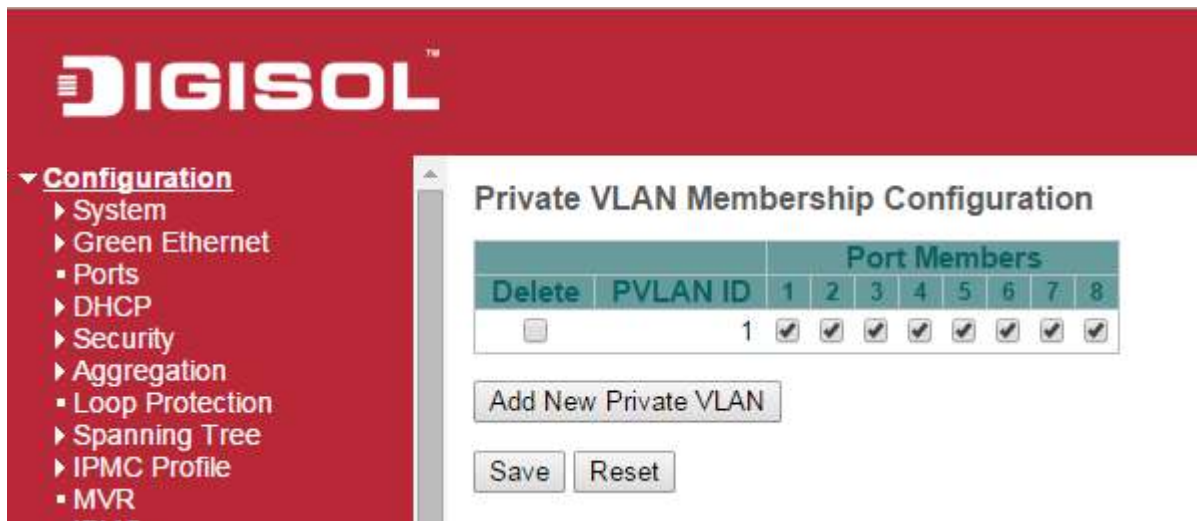
### 3.6.1 Membership

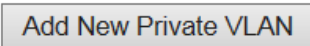
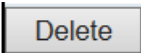
The [Private VLAN](#) membership configurations for the switch can be monitored and modified here. Private [VLANs](#) can be added or deleted here. Port members of each Private VLAN can be added or removed here.



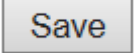
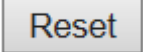
Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that [VLAN IDs](#) and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.



Object	Description
<b>Delete</b>	To delete a private VLAN entry, check this box. The entry will be deleted during the next save.
<b>PVLAN ID</b>	Indicates the ID of this particular private VLAN.
<b>Port members</b>	A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
<b>Adding a New Private VLAN</b>	<p>Click  to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction.</p> <p>The Private VLAN is enabled when you click "Save".</p> <p>The  button can be used to undo the addition of new Private VLANs.</p>

Buttons	
	Click to refresh the page immediately.
	Click to add a new private VLAN ID
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

### 3.6.2 Port Isolation

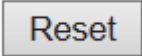
This page is used for enabling or disabling port isolation on ports in a [Private VLAN](#).

A port member of a [VLAN](#) can be isolated to other isolated ports on the same VLAN and Private VLAN.



Object	Description
<b>Port Members</b>	<p>A check box is provided for each port of a private VLAN.</p> <p>When checked, port isolation is enabled on that port.</p> <p>When unchecked, port isolation is disabled on that port.</p> <p>By default, port isolation is disabled on all ports.</p>


Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.
<input type="button" value="Save"/>	Click to save changes.

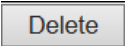
	Click to undo any changes made locally and revert to previously saved values.
---	---

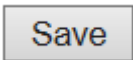
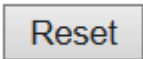
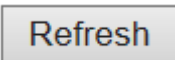
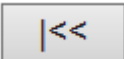

## 3.7 VCL

### 3.7.1 MAC-based VLAN

The MAC-based VLAN entries can be configured here. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

Object	Description
<b>Delete</b>	To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted in the stack.
<b>MAC Address</b>	Indicates the MAC address.
<b>VLAN ID</b>	Indicates the VLAN ID.
<b>Port Members</b>	A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
<b>Adding a New MAC-based VLAN</b>	Click  to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are <b>1</b> through <b>4095</b> .

	<p>The MAC-based VLAN entry is enabled when you click on "Save". A MAC-based VLAN without any port members will be deleted when you click "Save".</p> <p>The  button can be used to undo the addition of new MAC-based VLANs.</p> <p>The maximum possible MAC-based VLAN entries are limited to 256.</p>
--	---

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Refreshes the displayed table.
	Updates the table starting from the first entry in the MAC-based VLAN Table.
	Updates the table, starting with the entry after the last entry currently displayed.

### 3.7.2 Protocol-based VLAN

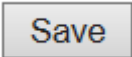
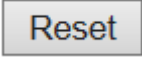
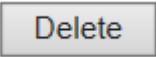


#### Protocol to Group

This page allows you to add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the switch.

Object	Description
<b>Delete</b>	To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.
<b>Frame Type</b>	<p>Frame Type can have one of the following values:</p> <p><b>Ethernet</b></p> <p><b>LLC</b></p> <p><b>SNAP</b></p> <p>Note: On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected.</p>
<b>Value</b>	<p>Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu.</p> <p>Below is the criteria for three different Frame Types:</p> <p><b>For Ethernet:</b> Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff</p>



	<p><b>For LLC:</b> Valid value in this case is comprised of two different sub-values.</p> <p>a. <b>DSAP:</b> 1-byte long string (0x00-0xff)</p> <p>b. <b>SSAP:</b> 1-byte long string (0x00-0xff)</p> <p><b>For SNAP:</b> Valid value in this case also is comprised of two different sub-values.</p> <p>a. <b>OUI:</b> OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.</p> <p>b. <b>PID:</b> If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.</p> <p>In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.</p>
<b>Group Name</b>	<p>A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers(0-9).</p> <p><b>Note:</b> special character and underscore(_) are not allowed.</p>

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.
	The button can be used to undo the addition of new entry. The maximum possible Protocol to Group mappings are limited to 128.
	Click to add a new entry in mapping table.
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Click to refresh the page immediately.

### 3.7.3 Group to VLAN

This page allows you to map a already configured Group Name to a [VLAN](#) for the switch.

**DIGISOL** **DG-IS4508HP**

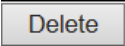
▼ **Configuration**

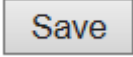
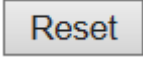

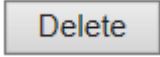
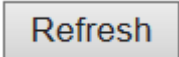
- ▶ System
- ▶ Green Ethernet
  - Ports
- ▶ DHCP
- ▶ Security
- ▶ Aggregation
  - Loop Protection
- ▶ Spanning Tree
- ▶ IPMC Profile
- MVR
- ▶ IPMC

**Group Name to VLAN mapping Table**

Delete	Group Name	VLAN ID	Port Members							
			1	2	3	4	5	6	7	8
No Group entries										

Object	Description
<b>Delete</b>	To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save.
<b>Group Name</b>	A valid Group Name is a string at the most 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers(0-9), no special character is allowed. whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be pre-used by any other existing mapping entry on this page.
<b>VLAN ID</b>	Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.
<b>Port Members</b>	A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
<b>Adding a New Group to VLAN mapping entry</b>	Click <input type="button" value="Add New Entry"/> to add a new entry in mapping table. An empty row is added to the table, the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are <b>1</b> through <b>4095</b> .

	<p>The  button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings are limited to 64.</p>
--	---


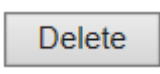
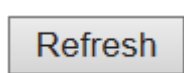
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.
	Click to add a new entry in mapping table. Legal values for a VLAN ID are <b>1</b> through <b>4095</b> .
	The button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings are limited to 64.
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Click to refresh the page immediately.

### 3.7.4 IP Subnet-based VLAN

The IP subnet-based VLAN entries can be configured here. This page allows for adding, updating and deleting IP subnet-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

Object	Description
<b>Delete</b>	To delete a IP subnet-based VLAN entry, check this box and press save. The entry will be deleted in the stack.
<b>VCE ID</b>	Indicates the index of the entry. It is user configurable. It's value ranges from 0-128. If a VCE ID is 0, application will auto-generate the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID.
<b>IP Address</b>	Indicates the IP address.
<b>Mask Length</b>	Indicates the network mask length.
<b>VLAN ID</b>	Indicates the VLAN ID. VLAN ID can be changed for the existing entries.
<b>Port Members</b>	A row of check boxes for each port is displayed for each IP subnet-based VLAN entry. To include a port in a IP subnet-based VLAN, check the box. To remove or exclude the port from the IP subnet-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.


Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

	Click to add a new IP subnet-based VLAN entry. Legal values for a VLAN ID are <b>1</b> through <b>4095</b> .
	The button can be used to undo the addition of new IP subnet-based VLANs. The maximum possible IP subnet-based VLAN entries are limited to 128.
<b>Auto-refresh</b> <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Refreshes the displayed table.

## 3.8 Voice VLAN

### 3.8.1 Voice VLAN Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the [IP](#) device to the switch, the IP phone should configure the voice [VLAN ID](#) correctly. It should be configured through its own GUI.


DG-IS4508HP

▼ Configuration

- ▶ System
- ▶ Green Ethernet
- Ports
- ▶ DHCP
- ▶ Security
- ▶ Aggregation
- Loop Protection
- ▶ Spanning Tree
- ▶ IPMC Profile
- MVR
- ▶ IPMC
- ▼ LLDP
  - LLDP
  - LLDP-MED
- ▼ PoE
  - PoE
  - Power Scheduler
  - Power Reset
- MAC Table
- VLANs
- ▼ Private VLANs
  - Membership
  - Port Isolation
- ▼ VCL
  - MAC-based VLAN
  - ▼ Protocol-based VLAN
    - Protocol to Group
    - Group to VLAN

### Voice VLAN Configuration

Mode	Disabled ▼
VLAN ID	1000
Aging Time	86400 seconds
Traffic Class	7 (High) ▼

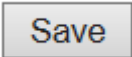
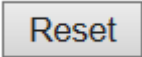
  

### Port Configuration

Port	Mode	Security	Discovery Protocol
*	<> ▼	<> ▼	<> ▼
1	Disabled ▼	Disabled ▼	OUI ▼
2	Disabled ▼	Disabled ▼	OUI ▼
3	Disabled ▼	Disabled ▼	OUI ▼
4	Disabled ▼	Disabled ▼	OUI ▼
5	Disabled ▼	Disabled ▼	OUI ▼
6	Disabled ▼	Disabled ▼	OUI ▼
7	Disabled ▼	Disabled ▼	OUI ▼
8	Disabled ▼	Disabled ▼	OUI ▼

Object	Description
<b>Mode</b>	Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are: <b>Enabled:</b> Enable Voice VLAN mode operation. <b>Disabled:</b> Disable Voice VLAN mode operation.
<b>VLAN ID</b>	Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is <b>1</b> to <b>4095</b> .
<b>Aging Time</b>	Indicates the Voice VLAN secure learning aging time. The allowed range is <b>10</b> to <b>10000000</b> seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.
<b>Traffic Class</b>	Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.
<b>Port Mode</b>	Indicates the Voice VLAN port mode. Possible port modes are:

	<p><b>Disabled:</b> Disjoin from Voice VLAN.</p> <p><b>Auto:</b> Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically.</p> <p><b>Forced:</b> Force join to Voice VLAN.</p>
<b>Port Security</b>	<p>Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds.</p> <p>Possible port modes are:</p> <p><b>Enabled:</b> Enable Voice VLAN security mode operation.</p> <p><b>Disabled:</b> Disable Voice VLAN security mode operation.</p>
<b>Port Discovery Protocol</b>	<p>Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are:</p> <p><a href="#">OUI</a>: Detect telephony device by OUI address.</p> <p><a href="#">LLDP</a>: Detect telephony device by LLDP.</p> <p><b>Both</b>: Both OUI and LLDP.</p>

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

### 3.8.2 Voice VLAN OUI

Configure VOICE VLAN OUI table on this page. The maximum number of entries is **16**.  
Modifying the OUI table will restart auto detection of OUI process.

**DIGISOL** **DG-IS4508HP**

**Configuration**

- System
- Green Ethernet
- Ports
- DHCP
- Security
- Aggregation
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
  - LLDP
  - LLDP-MED
- PoE
  - PoE
  - Power Scheduler
  - Power Reset

**Voice VLAN OUI Table**

Delete	Telephony OUI	Description
<input type="checkbox"/>	00-01-e3	Siemens AG phones
<input type="checkbox"/>	00-03-6b	Cisco phones
<input type="checkbox"/>	00-0f-e2	H3C phones
<input type="checkbox"/>	00-60-b9	Philips and NEC AG phones
<input type="checkbox"/>	00-d0-1e	Pingtel phones
<input type="checkbox"/>	00-e0-75	Polycom phones
<input type="checkbox"/>	00-e0-bb	3Com phones

Object	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>Telephony OUI</b>	A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).
<b>Description</b>	The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is <b>0</b> to <b>32</b> .

Buttons	
<input type="button" value="Add New Entry"/>	Click to add a new access management entry.
<input type="button" value="Save"/>	Click to save changes.



<div data-bbox="272 264 413 320" data-label="Text">Reset</div>	Click to undo any changes made locally and revert to previously saved values.
--	---

## 3.9 QoS

### 3.9.1 Port Classification

This page allows you to configure the basic [QoS](#) Ingress Classification settings for all switch ports.

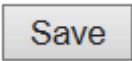
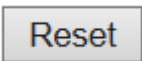
The screenshot shows the DIGISOL DG-IS4508HP Industrial switch configuration interface. On the left is a navigation menu with the following items: Configuration, System, Green Ethernet, Ports, DHCP, Security, Aggregation, Loop Protection, Spanning Tree, IPMC Profile, MVR, IPMC, LLDP, PoE, MAC Table, VLANs, Private VLANs, VCL, and Voice VLAN. The main content area is titled "QoS Ingress Port Classification" and contains a table with the following columns: Port, CoS, DPL, PCP, DEI, Tag Class., DSCP Based, and Address Mode. The table has 8 rows, one for each port (1-8). Each row contains dropdown menus for Port, CoS, DPL, PCP, and DEI, and checkboxes for Tag Class. and DSCP Based. The Address Mode column contains dropdown menus. Below the table are "Save" and "Reset" buttons.

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Address Mode
*	<>	<>	<>	<>		<input type="checkbox"/>	<>
1	0	0	0	0	Disabled	<input type="checkbox"/>	Source
2	0	0	0	0	Disabled	<input type="checkbox"/>	Source
3	0	0	0	0	Disabled	<input type="checkbox"/>	Source
4	0	0	0	0	Disabled	<input type="checkbox"/>	Source
5	0	0	0	0	Disabled	<input type="checkbox"/>	Source
6	0	0	0	0	Disabled	<input type="checkbox"/>	Source
7	0	0	0	0	Disabled	<input type="checkbox"/>	Source
8	0	0	0	0	Disabled	<input type="checkbox"/>	Source

Object	Description
<b>Port</b>	The port number for which the configuration below applies.
<b>CoS</b>	<p>Controls the default class of service.</p> <p>All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority.</p>

	<p>If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS.</p> <p>The classified CoS can be overruled by a QCL entry.</p> <p><b>Note:</b> If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.</p>
<b>DPL</b>	<p>Controls the default <a href="#">drop precedence level</a>.</p> <p>All frames are classified to a drop precedence level.</p> <p>If the port is VLAN aware and the frame is tagged, then the frame is classified to a DPL that is equal to the DEI value in the tag. Otherwise the frame is classified to the default DPL.</p> <p>If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL.</p> <p>The classified DPL can be overruled by a QCL entry.</p>
<b>PCP</b>	<p>Controls the default <a href="#">PCP</a> value.</p> <p>All frames are classified to a PCP value.</p> <p>If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.</p>
<b>DEI</b>	<p>Controls the default <a href="#">DEI</a> value.</p> <p>All frames are classified to a DEI value.</p> <p>If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.</p>
<b>Tag Class.</b>	<p>Shows the classification mode for tagged frames on this port.</p> <p><b>Disabled:</b> Use default CoS and DPL for tagged frames.</p> <p><b>Enabled:</b> Use mapped versions of <a href="#">PCP</a> and <a href="#">DEI</a> for tagged frames.</p>

	<p>Click on the mode in order to configure the mode and/or mapping.</p> <p><b>Note:</b> This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.</p>
<b>DSCP Based</b>	Click to Enable <a href="#">DSCP</a> Based QoS Ingress Port Classification.
<b>Address Mode</b>	<p>The IP/MAC address mode specifying whether the <a href="#">QCL</a> classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are:</p> <p><b>Source:</b> Enable SMAC/SIP matching.</p> <p><b>Destination:</b> Enable DMAC/DIP matching.</p>

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

### 3.9.2 Port Policing

This page allows you to configure the [Policer](#) settings for all switch ports.

**DIGISOL™** **DG-IS4508HP**

▼ **Configuration**

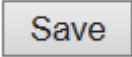
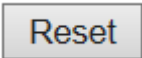
- ▶ System
- ▶ Green Ethernet
- ▶ Ports
- ▶ DHCP
- ▶ Security
- ▶ Aggregation
- ▶ Loop Protection
- ▶ Spanning Tree
- ▶ IPMC Profile
- ▶ MVR
- ▶ IPMC
- ▶ LLDP
- ▶ PoE
- ▶ MAC Table
- ▶ VLANs
- ▶ Private VLANs
- ▶ VCL
- ▶ Voice VLAN

#### QoS Ingress Port Policers

Port	Enabled	Rate	Unit	Flow Control
*	<input type="checkbox"/>	500	<> ▼	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
2	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
3	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
7	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
8	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>

Object	Description
<b>Port</b>	The port number for which the configuration below applies.
<b>Enabled</b>	Controls whether the policer is enabled on this switch port.
<b>Rate</b>	Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-3300 when the "Unit" is "Mbps" or "kfps".
<b>Unit</b>	Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is "kbps".
<b>Flow Control</b>	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

#### Buttons

	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

### 3.9.3 Port Scheduler

This page provides an overview of QoS Egress Port Schedulers for all switch ports.

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-

Object	Description
<b>Port</b>	The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.
<b>Mode</b>	Shows the scheduling mode for this port.
<b>Qn</b>	Shows the weight for this queue and port.

### 3.9.4 Port Shaping

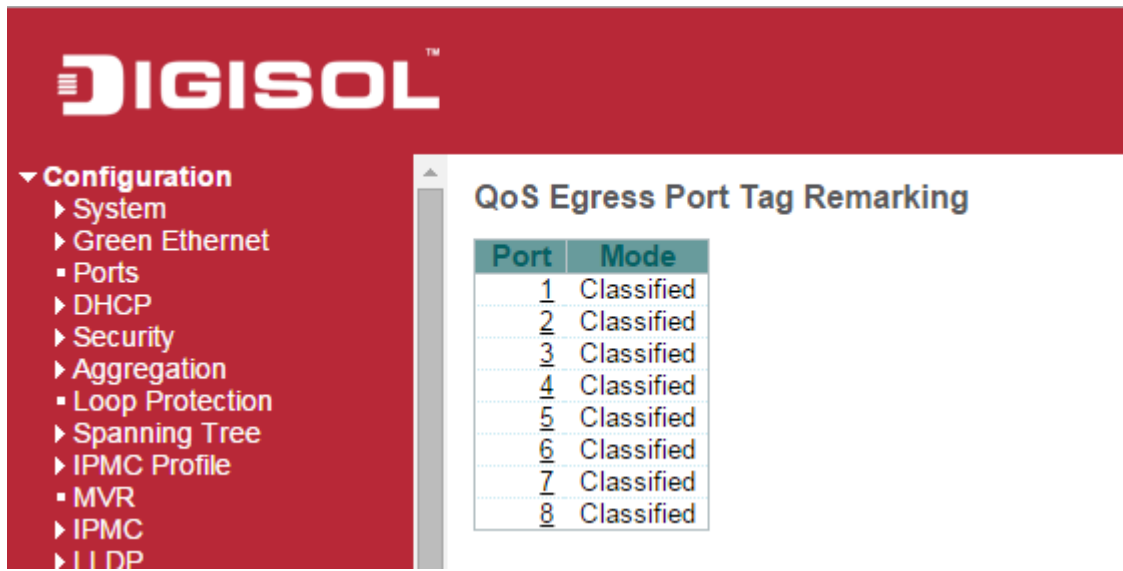
This page provides an overview of QoS Egress Port Shapers for all switch ports.

Port	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

Object	Description
<b>Port</b>	The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.
<b>Qn</b>	Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps".
<b>Port #</b>	Shows "disabled" or actual port shaper rate - e.g. "800 Mbps".

### 3.9.5 Port Tag Remarking

This page provides an overview of [QoS](#) Egress Port Tag Remarking for all switch ports.



Object	Description
<b>Port</b>	The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking.
<b>Mode</b>	Shows the tag remarking mode for this port. <b>Classified:</b> Use classified <a href="#">PCP/DEI</a> values. <b>Default:</b> Use default PCP/DEI values. <b>Mapped:</b> Use mapped versions of <a href="#">QoS class</a> and <a href="#">DP level</a> .



### 3.9.6 Port DSCP

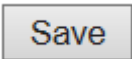

This page allows you to configure the basic [QoS](#) Port [DSCP](#) Configuration settings for all switch ports.

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	<input type="checkbox"/>	<>	<>
1	<input type="checkbox"/>	Disable	Disable
2	<input type="checkbox"/>	Disable	Disable
3	<input type="checkbox"/>	Disable	Disable
4	<input type="checkbox"/>	Disable	Disable
5	<input type="checkbox"/>	Disable	Disable
6	<input type="checkbox"/>	Disable	Disable
7	<input type="checkbox"/>	Disable	Disable
8	<input type="checkbox"/>	Disable	Disable

Save Reset

Object	Description
<b>Port</b>	The Port column shows the list of ports for which you can configure dscp ingress and egress settings.
<b>Ingress</b>	<p>In Ingress settings you can change ingress translation and classification settings for individual ports.</p> <p>There are two configuration parameters available in Ingress:</p> <p><b>Translate</b></p> <p><b>Classify</b></p>
<b>Translate</b>	To Enable the Ingress Translation click the checkbox.
<b>Classify</b>	Classification for a port have 4 different values.

	<p><b>-Disable:</b> No Ingress DSCP Classification.</p> <p><b>-DSCP=0:</b> Classify if incoming (or translated if enabled) DSCP is 0.</p> <p><b>-Selected:</b> Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.</p> <p><b>-All:</b> Classify all DSCP.</p>
<b>Egress</b>	<p>Port Egress Rewriting can be one of -</p> <p><b>-Disable:</b> No Egress rewrite.</p> <p><b>-Enable:</b> Rewrite enabled without remapping.</p> <p><b>-Remap DP Unaware:</b> DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation-&gt;Egress Remap DP0' table.</p> <p><b>-Remap DP Aware:</b> DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation-&gt;Egress Remap DP0' table or from the 'DSCP Translation-&gt;Egress Remap DP1' table.</p>

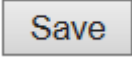
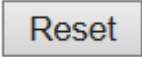
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

### 3.9.7 DSCP-Based QoS

This page allows you to configure the basic [QoS DSCP](#) based QoS Ingress Classification settings for all switches.

DSCP	Trust	QoS Class	DPL
*	<input type="checkbox"/>	<>	<>
0 (BE)	<input type="checkbox"/>	0	0
1	<input type="checkbox"/>	0	0
2	<input type="checkbox"/>	0	0
3	<input type="checkbox"/>	0	0
4	<input type="checkbox"/>	0	0
5	<input type="checkbox"/>	0	0
6	<input type="checkbox"/>	0	0
7	<input type="checkbox"/>	0	0
8 (CS1)	<input type="checkbox"/>	0	0
9	<input type="checkbox"/>	0	0
10 (AF11)	<input type="checkbox"/>	0	0
11	<input type="checkbox"/>	0	0
12 (AF12)	<input type="checkbox"/>	0	0
13	<input type="checkbox"/>	0	0
14 (AF13)	<input type="checkbox"/>	0	0
15	<input type="checkbox"/>	0	0
16 (CS2)	<input type="checkbox"/>	0	0
17	<input type="checkbox"/>	0	0
18 (AF21)	<input type="checkbox"/>	0	0

Object	Description
<b>DSCP</b>	Maximum number of supported DSCP values are 64.
<b>Trust</b>	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific <a href="#">QoS class</a> and <a href="#">Drop Precedence Level</a> . Frames with untrusted DSCP values are treated as a non-IP frame.
<b>QoS Class</b>	QoS class value can be any of (0-7)
<b>DPL</b>	Drop Precedence Level (0-1)

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.



### 3.9.8 DSCP Translation

This page allows you to configure the basic [QoS DSCP](#) Translation settings for all switches. DSCP translation can be done in Ingress or Egress.

**DIGISOL™** **DG-IS4508HP Industrial Ethernet Switch**

**Configuration**

- System
- Green Ethernet
- Ports
- DHCP
- Security
- Aggregation
  - Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- PoE
- MAC Table
- VLANs
  - Private VLANs
- VCL
- Voice VLAN
- QoS
  - Port Classification
  - Port Policing
  - Port Scheduler
  - Port Shaping
  - Port Tag Remarking
  - Port DSCP
  - DSCP-Based QoS
  - DSCP Translation
  - DSCP Classification
  - QoS Control List
  - Storm Control
- Mirroring
- GVRP
- sFlow
- RingV2
- DDMI

**Monitor**

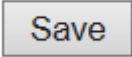
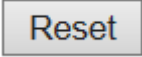
- System

**DSCP Translation**

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	<input type="checkbox"/>	<>	<>
0 (BE)	0 (BE)	<input type="checkbox"/>	0 (BE)	0 (BE)
1	1	<input type="checkbox"/>	1	1
2	2	<input type="checkbox"/>	2	2
3	3	<input type="checkbox"/>	3	3
4	4	<input type="checkbox"/>	4	4
5	5	<input type="checkbox"/>	5	5
6	6	<input type="checkbox"/>	6	6
7	7	<input type="checkbox"/>	7	7
8 (CS1)	8 (CS1)	<input type="checkbox"/>	8 (CS1)	8 (CS1)
9	9	<input type="checkbox"/>	9	9
10 (AF11)	10 (AF11)	<input type="checkbox"/>	10 (AF11)	10 (AF11)
11	11	<input type="checkbox"/>	11	11
12 (AF12)	12 (AF12)	<input type="checkbox"/>	12 (AF12)	12 (AF12)
13	13	<input type="checkbox"/>	13	13
14 (AF13)	14 (AF13)	<input type="checkbox"/>	14 (AF13)	14 (AF13)
15	15	<input type="checkbox"/>	15	15
16 (CS2)	16 (CS2)	<input type="checkbox"/>	16 (CS2)	16 (CS2)
17	17	<input type="checkbox"/>	17	17
18 (AF21)	18 (AF21)	<input type="checkbox"/>	18 (AF21)	18 (AF21)
19	19	<input type="checkbox"/>	19	19
20 (AF22)	20 (AF22)	<input type="checkbox"/>	20 (AF22)	20 (AF22)
21	21	<input type="checkbox"/>	21	21

Object	Description
<b>DSCP</b>	Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.
<b>Ingress</b>	Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.  There are two configuration parameters for DSCP Translation - <b>Translate</b> <b>Classify</b>
<b>Translation</b>	DSCP at Ingress side can be translated to any of (0-63) DSCP values.
<b>Classify</b>	Click to enable Classification at Ingress side.
<b>Egress</b>	There are the following configurable parameters for Egress side -

	<p><b>Remap DP0</b> Controls the remapping for frames with DP level 0.</p> <p><b>Remap DP1</b> Controls the remapping for frames with DP level 1.</p>
<b>Remap DP0</b>	Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.
<b>Remap DP1</b>	Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

### 3.9.9 DSCP Classification

This page allows you to configure the mapping of [QoS class](#) and [Drop Precedence Level](#) to [DSCP](#) value.

**DIGISOL™** **DG-IS4508HP**

▼ **Configuration**

- ▶ System
- ▶ Green Ethernet
  - Ports
- ▶ DHCP
- ▶ Security
- ▶ Aggregation
  - Loop Protection
- ▶ Spanning Tree
- ▶ IPMC Profile
- MVR
- ▶ IPMC
- ▶ LLDP
- ▶ PoE
  - MAC Table
- VLANs
  - ▶ Private VLANs
- ▶ VCL
- ▶ Voice VLAN
- ▼ **QoS**
  - Port Classification
  - Port Policing
  - Port Scheduler
  - Port Shaping
  - Port Tag Remark
  - Port DSCP
  - DSCP-Based QoS
  - DSCP Translation

**DSCP Classification**

QoS Class	DPL	DSCP
*	*	<> ▼
0	0	0 (BE) ▼
0	1	0 (BE) ▼
1	0	0 (BE) ▼
1	1	0 (BE) ▼
2	0	0 (BE) ▼
2	1	0 (BE) ▼
3	0	0 (BE) ▼
3	1	0 (BE) ▼
4	0	0 (BE) ▼
4	1	0 (BE) ▼
5	0	0 (BE) ▼
5	1	0 (BE) ▼
6	0	0 (BE) ▼
6	1	0 (BE) ▼
7	0	0 (BE) ▼
7	1	0 (BE) ▼

Save Reset

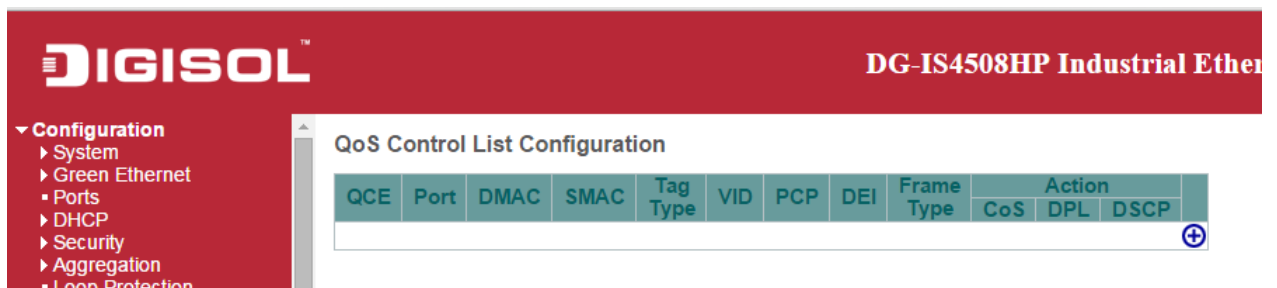
Object	Description
<b>QoS Class</b>	Actual QoS class.
<b>DPL</b>	Actual Drop Precedence Level.
<b>DSCP</b>	Select the classified DSCP value (0-63).

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

### 3.9.10 QoS Control List







This page shows the QoS Control List([QCL](#)), which is made up of the [QCE](#)s. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch.

Click on the lowest plus sign to add a new QCE to the list.

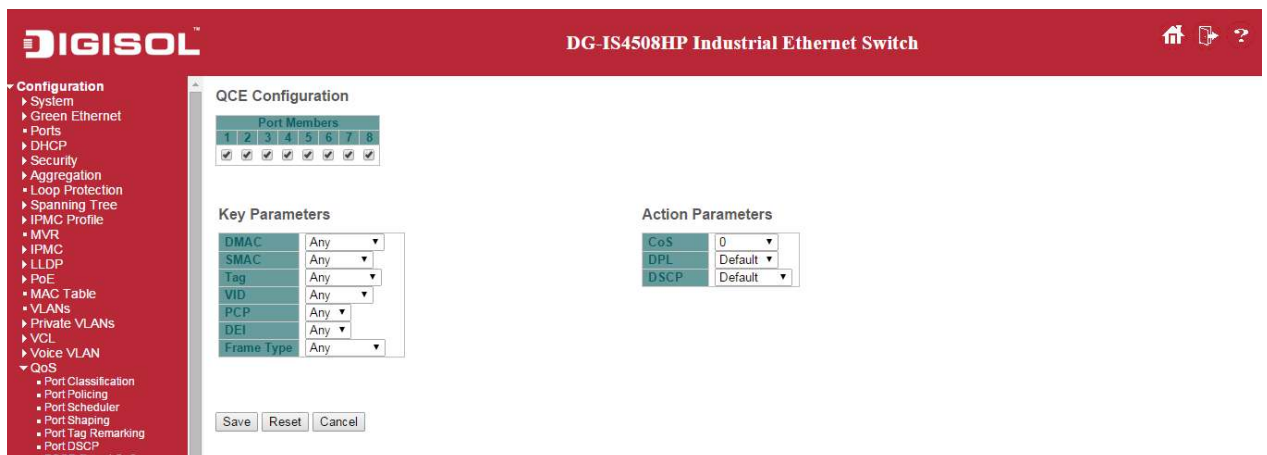


Object	Description
<b>QCE</b>	Indicates the QCE id.
<b>Port</b>	Indicates the list of ports configured with the QCE.
<b>DMAC</b>	<p>Indicates the destination MAC address. Possible values are:</p> <p><b>Any</b>: Match any DMAC.</p> <p><b>Unicast</b>: Match unicast DMAC.</p> <p><b>Multicast</b>: Match multicast DMAC.</p> <p><b>Broadcast</b>: Match broadcast DMAC.</p> <p>The default value is 'Any'.</p>
<b>SMAC</b>	<p>Match specific source MAC address or 'Any'.</p> <p>If a port is configured to match on DMAC/DIP, this field indicates the DMAC.</p>
<b>Tag Type</b>	<p>Indicates tag type. Possible values are:</p> <p><b>Any</b>: Match tagged and untagged frames.</p> <p><b>Untagged</b>: Match untagged frames.</p>



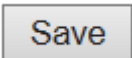
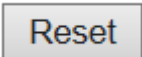
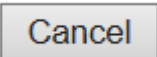
	<p><b>Tagged:</b> Match tagged frames.</p> <p>The default value is 'Any'.</p>
<b>VID</b>	Indicates ( <a href="#">VLAN ID</a> ), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'
<b>PCP</b>	Priority Code Point: Valid values of PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
<b>DEI</b>	Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.
<b>Frame Type</b>	<p>Indicates the type of frame. Possible values are:</p> <p><b>Any:</b> Match any frame type.</p> <p><b>Ethernet:</b> Match EtherType frames.</p> <p><b>LLC:</b> Match (<a href="#">LLC</a>) frames.</p> <p><b>SNAP:</b> Match (<a href="#">SNAP</a>) frames.</p> <p><b>IPv4:</b> Match IPv4 frames.</p> <p><b>IPv6:</b> Match IPv6 frames.</p>
<b>Action</b>	<p>Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.</p> <p>Possible actions are:</p> <p><b>CoS:</b> Classify <a href="#">Class of Service</a>.</p> <p><b>DPL:</b> Classify <a href="#">Drop Precedence Level</a>.</p> <p><b>DSCP:</b> Classify <a href="#">DSCP</a> value.</p>
<b>Modification Buttons</b>	<p>You can modify each QCE (QoS Control Entry) in the table using the following buttons:</p> <p>: Inserts a new QCE before the current row.</p> <p>: Edits the QCE.</p> <p>: Moves the QCE up the list.</p> <p>: Moves the QCE down the list.</p> <p>: Deletes the QCE.</p> <p>: The lowest plus sign adds a new entry at the bottom of the QCE listings.</p>

The QCE page includes the following fields:



Object	Description
<b>Port Members</b>	Check the checkbox button to include the port in the QCL entry. By default all ports are included.
<b>Key parameters</b>	<p>Key configuration is described as below:</p> <p><b>DMAC</b> Destination MAC address: Possible values are 'Unicast', 'Multicast', 'Broadcast' or 'Any'.</p> <p><b>SMAC</b> Source MAC address: xx-xx-xx-xx-xx-xx or 'Any'. If a port is configured to match on DMAC/DIP, this field is the Destination MAC address.</p> <p><b>Tag</b> Value of Tag field can be 'Untagged', 'Tagged' or 'Any'.</p> <p><b>VID</b> Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.</p> <p><b>PCP</b> Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.</p> <p><b>DEI</b> Valid value of DEI can be '0', '1' or 'Any'.</p> <p><b>Frame Type</b> Frame Type can have any of the following values:</p> <p><b>Any:</b> Allow all types of frames.</p> <p><b>EtherType: Ether Type</b> Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'.</p> <p><b>LLC: SSAP Address</b> Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'.</p> <p><b>DSAP Address</b> Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'.</p> <p><b>Control</b> Valid Control field can vary from 0x00 to 0xFF or 'Any'.</p>

	<p><b>SNAP: PID</b> Valid PID(a.k.a Ether Type) can be 0x0000-0xFFFF or 'Any'.</p> <p><b>IPv4: Protocol</b> IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.</p> <p><b>Source IP</b> Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero. If a port is configured to match on DMAC/DIP, this field is the Destination IP address.</p> <p><b>IP Fragment</b> IPv4 frame fragmented option: 'Yes', 'No' or 'Any'.</p> <p><b>DSCP</b> Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.</p> <p><b>Sport</b> Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.</p> <p><b>Dport</b> Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.</p> <p><b>IPv6: Protocol</b> IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.</p> <p><b>Source IP</b> 32 LS bits of IPv6 source address in value/mask format or 'Any'. If a port is configured to match on DMAC/DIP, this field is the Destination IP address.</p> <p><b>DSCP</b> Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.</p> <p><b>Sport</b> Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.</p> <p><b>Dport</b> Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.</p>
<b>Action Parameters</b>	<p><b>CoS</b> <a href="#">Class of Service</a>: (0-7) or 'Default'.</p> <p><b>DP</b> <a href="#">Drop Precedence Level</a>: (0-1) or 'Default'.</p> <p><b>DSCP</b> <a href="#">DSCP</a>: (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.</p> <p>'Default' means that the default classified value is not modified by this QCE.</p>

Buttons	
	Click to save the configuration and move to main QCL page.
	Click to undo any changes made locally and revert to previously saved values.
	Return to the previous page without saving the configuration change.

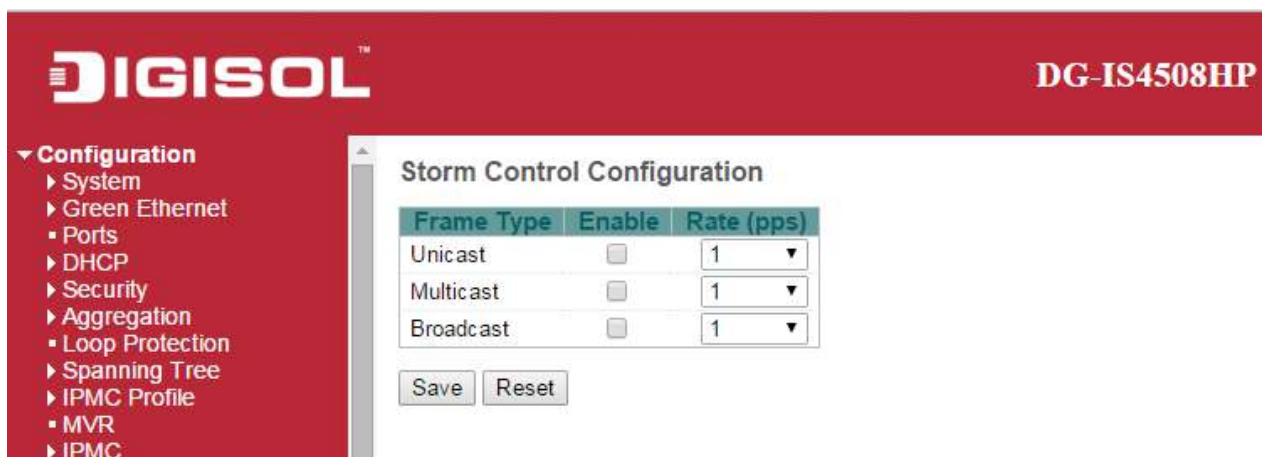


### 3.9.11 Storm Control

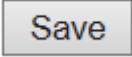
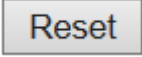
Storm control for the switch is configured on this page.

There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch.



Object	Description
<b>Frame Type</b>	The settings in a particular row apply to the frame type listed here: Unicast, Multicast or Broadcast.
<b>Enable</b>	Enable or disable the storm control status for the given frame type.
<b>Rate</b>	The rate unit is packets per second (pps). Valid values are: <b>1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K</b> or <b>1024K</b> .

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

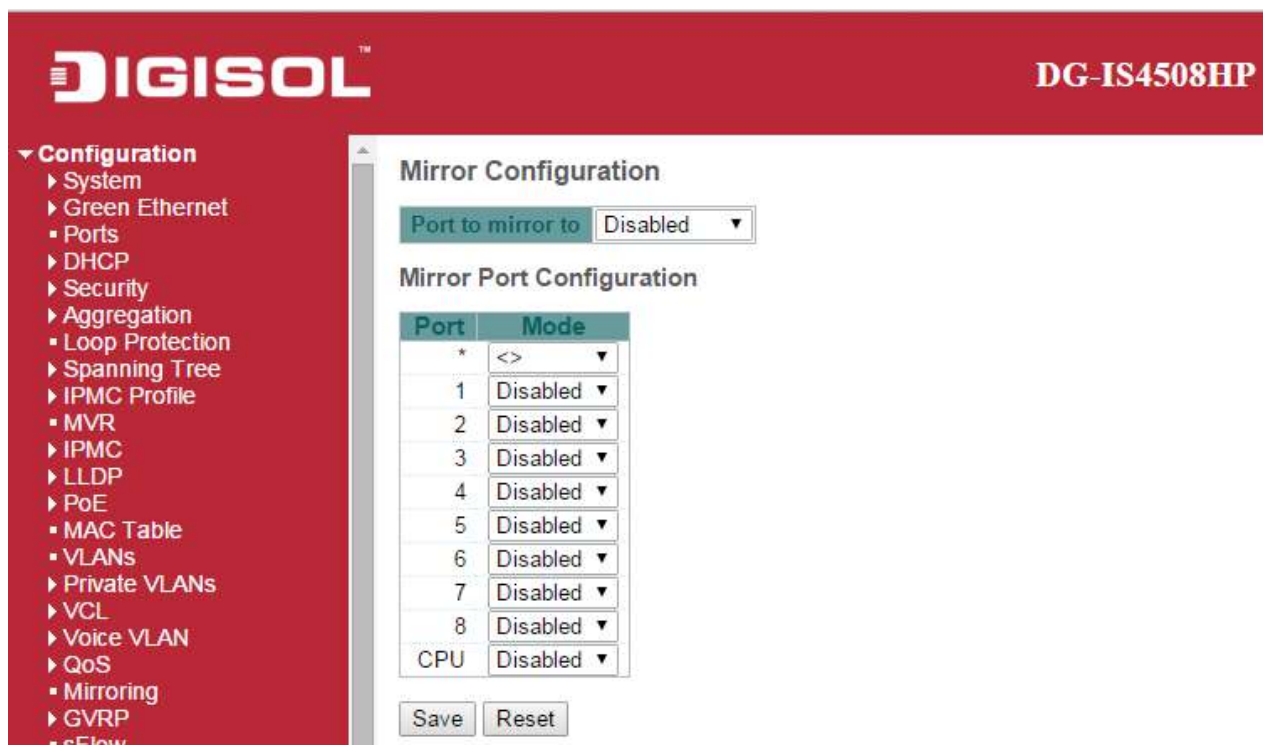
## 4.0 Mirroring

Configure port [Mirroring](#) on this page.

To debug network problems, selected traffic can be copied, or mirrored, on a **mirror port** where a frame analyzer can be attached to analyze the frame flow.

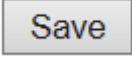
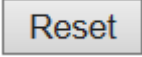
The traffic to be copied on the **mirror port** is selected as follows:

- All frames received on a given port (also known as ingress or source mirroring).
- All frames transmitted on a given port (also known as egress or destination mirroring).



Object	Description
Port to mirror	Port to mirror also known as the <b>mirror port</b> . Frames from ports that have either

	source (rx) or destination (tx) mirroring enabled are mirrored on this port. <b>Disabled</b> disables mirroring.
<b>Port</b>	The logical port for the settings contained in the same row.
<b>Mode</b>	<p>Select mirror mode.</p> <p><b>Rx only</b> Frames received on this port are mirrored on the <b>mirror port</b>. Frames transmitted are not mirrored.</p> <p><b>Tx only</b> Frames transmitted on this port are mirrored on the <b>mirror port</b>. Frames received are not mirrored.</p> <p><b>Disabled</b> Neither frames transmitted nor frames received are mirrored.</p> <p><b>Enabled</b> Frames received and frames transmitted are mirrored on the <b>mirror port</b>.</p> <p>Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror <b>mirror port</b> Tx frames. Because of this, <b>mode</b> for the selected <b>mirror port</b> is limited to <b>Disabled</b> or <b>Rx only</b>.</p>

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.



## 5.0 GVRP

### 5.1 Global Config

This page allows you to configure the basic [GVRP](#) Configuration settings for all switch ports.

**DIGISOL™** DG-IS4508HP Industrial Ethernet Switch

**Configuration**

- System
- Green Ethernet
- Ports
- DHCP
- Security
- Aggregation
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- PoE

**GVRP Configuration**

☐ Enable GVRP

Parameter	Value
Join-time:	20
Leave-time:	60
LeaveAll-time:	1000
Max VLANs:	20

Object	Description
<b>GVRP Protocol timers</b>	<p>Join-time is a value in the range 1-20 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 20.</p> <p>Leave-time is a value in the range 60-300 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 60.</p> <p>LeaveAll-time is a value in the range 1000-5000 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 1000.</p>
<b>Max number of VLANs</b>	When GVRP is enabled a maximum number of VLANs supported by GVRP is specified. By default this number is 20. This number can only be changed when GVRP is turned off.

Buttons	
<input type="button" value="Save"/>	Click to save changes.

## 5.2 Port Config

This page allows you to enable a port for GVRP.

**DIGISOL™** **DG-IS4508HP**

▼ **Configuration**

- ▶ System
- ▶ Green Ethernet
- ▶ Ports
- ▶ DHCP
- ▶ Security
- ▶ Aggregation
- ▶ Loop Protection
- ▶ Spanning Tree
- ▶ IPMC Profile
- ▶ MVR
- ▶ IPMC
- ▶ LLDP
- ▶ PoE
- ▶ MAC Table
- ▶ VLANs
- ▶ Private VLANs
- ▶ VCI

### GVRP Port Configuration

Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled

Buttons	
<input type="button" value="Save"/>	Click to save changes.

## 6.0 sFlow

This page allows for configuring [sFlow](#). The configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.

sFlow configuration is not persisted to non-volatile memory, which means that a reboot will disable sFlow sampling.

The screenshot shows the DIGISOL web interface for the DG-IS4508HP Industrial Ethernet Switch. The left sidebar contains a navigation menu with categories like Configuration, Monitor, Diagnostics, and Maintenance. The main content area is titled 'sFlow Configuration' and includes a 'Refresh' button. It is divided into three sections: Agent Configuration, Receiver Configuration, and Port Configuration.

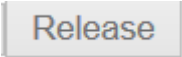
**Agent Configuration:** IP Address is set to 127.0.0.1.

**Receiver Configuration:** Owner is <none> (with a Release button), IP Address/Hostname is 0.0.0.0, UDP Port is 6343, Timeout is 0 seconds, and Max. Datagram Size is 1400 bytes.


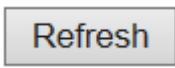
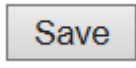
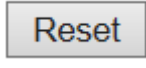
**Port Configuration:** A table showing ports 1 through 8. Each port has an 'Enabled' checkbox, a 'Flow Sampler' section (Sampling Rate and Max. Header), and a 'Counter Poller' section (Enabled checkbox and Interval).

Port	Enabled	Flow Sampler		Counter Poller	
		Sampling Rate	Max. Header	Enabled	Interval
*	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
1	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
2	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
3	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
4	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
5	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
6	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
7	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
8	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0

Buttons: Save, Reset

Object	Description
<b>Agent Configuration</b>	
<b>IP Address</b>	<p>The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time.</p> <p>Both IPv4 and IPv6 addresses are supported.</p>
<b>Receiver Configuration</b>	
<b>Owner</b>	<p>Basically, sFlow can be configured in two ways: Through local management using the Web or CLI interface or through <a href="#">SNMP</a>. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:</p> <ul style="list-style-type: none"> <li>• If sFlow is currently unconfigured/unclaimed, Owner contains <b>&lt;none&gt;</b>.</li> <li>• If sFlow is currently configured through Web or CLI, Owner contains <b>&lt;Configured through local management&gt;</b>.</li> <li>• If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.</li> </ul> <p>If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.</p> <p>The  button allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).</p>
<b>IP Address/Hostname</b>	The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are

	supported.
<b>UDP Port</b>	The <a href="#">UDP</a> port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.
<b>Timeout</b>	The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings.
<b>Max. Datagram Size</b>	The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.
<b>Port Configuration</b>	
<b>Port</b>	The port number for which the configuration below applies.
<b>Flow Sampler Enabled</b>	Enables/disables flow sampling on this port.
<b>Flow Sampler Sampling Rate</b>	The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port.  Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field.
<b>Flow Sampler Max. Header</b>	The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes.  If the <a href="#">maximum datagram size</a> does not take into account the maximum header size, samples may be dropped.
<b>Counter Poller Enabled</b>	Enables/disables counter polling on this port.
<b>Counter Poller Interval</b>	With counter polling enabled, this specifies the interval - in seconds - between counter poller samples.

<b>Buttons</b>	
	See description under <a href="#">Owner</a> .
	Click to refresh the page. Note that unsaved changes will be lost.
	Click to save changes. Note that sFlow configuration is not persisted to non-volatile memory.
	Click to undo any changes made locally and revert to previously saved values.



## 7.0 RingV2

This page provides Ring related configuration.

**DIGISOL™** **DG-IS4508HP Industrial**

▼ **Configuration**

- ▶ System
- ▶ Green Ethernet
- Ports
- ▶ DHCP
- ▶ Security
- ▶ Aggregation
- Loop Protection
- ▶ Spanning Tree
- ▶ IPMC Profile
- MVR
- ▶ IPMC
- ▶ LLDP
- ▶ PoE
- MAC Table
- VLANs
- ▶ Private VLANs
- ▶ VCL
- ▶ Voice VLAN
- ▶ QoS

### RingV2 Configuration

Ring Configuration

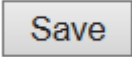
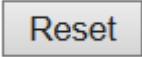
Index	Mode	Role	Ring Port(s)
1	Disable ▼	Ring(Slave) ▼	Forward Port : Port-1 ▼ Forward Port : Port-2 ▼
2	Disable ▼	Ring(Slave) ▼	Forward Port : Port-3 ▼ Forward Port : Port-4 ▼
3	Disable ▼	Chain(Member) ▼	Member Port : Port-1 ▼ Member Port : Port-2 ▼

Save Reset

Object	Description
<b>Index</b>	<p>The group index. This parameter is used for easy identifying the ring when user configure it.</p> <p>Group 1 (Index 1) - It supports configuration of ring.</p> <p>Group 2 (Index 2) - It supports configuration of ring, coupling and dual-homing.</p> <p>Group 3 (Index 3) - It supports configuration of chain and balancing-chain.</p>
<b>Mode</b>	<p>Enable Ring on the specific group.</p> <p>When Group 1 or 2 is enabled, all configuration of Group 3 will be reset to default. Group 3 all configuration options will be locked.</p> <p>To configure Group 3, both Group1 and 2 should be disabled first. When Group 3 is enabled, all configuration of Group1 and 2 will be reset to default. Group 1 and 2 all configuration options will be locked.</p>
<b>Role</b>	Configure the Ring group on this switch as specific role.

	<p>Group 1 - support option of ring-master and ring-slave.</p> <p># Ring - it could be master or slave.</p> <p>Group 2 - support configuration of the ring, coupling and dual-homing.</p> <p># Ring - it could be master or slave.</p> <p># Coupling - it could be primary and backup.</p> <p># Dual-Homing</p> <p>Group 3 - support configuration of the chain and balancing-chain.</p> <p># Chain - it could be head, tail or member.</p> <p># Balancing Chain - it could be central-block, terminal-1/2 or member.</p> <p>Note 1 - Group 1 must be enabled before enable Group 2 to coupling.</p> <p>Note 2 - When Group 1 or 2 is enabled, the configuration of Group 3 will be disabled.</p> <p>Note 3 - When Group 3 is enabled, the configuration of Group 1 and 2 will be disabled.</p>
<b>Ring Port(s)</b>	<p>Selecting ring port(s).</p> <p>Each ring port must be unique, CANNOT be configured in different groups; 2 ring ports between ring/chain CANNOT be the same.</p> <p># When role is ring/master, one ring port is <b>forward port</b> and another is <b>block port</b>. The block port is redundant port; it is blocking port in normal state.</p> <p># When role is ring/slave, both ring ports are <b>forward port</b>.</p> <p># When role is coupling/primary, only need one ring port named <b>primary port</b>.</p> <p># When role is coupling/backup, only need one ring port named <b>backup port</b>. This backup port is redundant port; it is blocking port in normal state.</p> <p># When role is dual-homing, one ring port is <b>primary port</b> and another is <b>backup port</b>. This backup port is redundant port; it is blocking port in normal state.</p> <p># When role is chain/head, one ring port is <b>member port</b> and another is <b>head port</b>. Both ring ports are forwarding port in normal state.</p>

	<p># When role is chain/tail, one ring port is <b>member port</b> and another is <b>tail port</b>. The tail port is redundant port; it is blocking port in normal state.</p> <p># When role is chain/member, both ring ports are <b>member port</b>. Both ring ports are forwarding port in normal state.</p> <p># When role is balancing-chain/central-block, one ring port is <b>member port</b> and another is <b>block port</b>. The block port is redundant port; it is blocking port in normal state.</p> <p># When role is balancing-chain/terminal-1/2, one ring port is <b>member port</b> and another is <b>terminal port</b>. Both ring ports are forwarding port in normal state.</p> <p># When role is balancing-chain/member, both ring ports are <b>member port</b>. Both ring ports are forwarding port in normal state.</p>
--	--

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

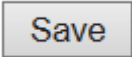
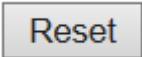


## 8.0 DDM

Configure DDMI on this page.



Object	Description
<b>Mode</b>	
<b>Enabled</b>	Enable DDMI mode operation.
<b>Disabled</b>	Disable DDMI mode operation.

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

## Monitor

### System

### System Information

The switch system information is provided here.

**DIGISOL™** **DG-IS4508HP**


**Configuration**

- System
- Green Ethernet
- Ports
- DHCP
- Security
- Aggregation
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- LLDP
- PoE
- MAC Table
- VLANs
- Private VLANs
- VCL

**System Information**

System	
Contact	
Name	
Location	
Hardware	
MAC Address	00-17-7c-6a-bd-72
Chip ID	VSC7425
Time	
System Date	2000-01-01T05:50:55+00:00
System Uptime	0d 05:50:57
Software	
Software Version	v00.00.01B15
Software Date	2016-08-02T10:38:31+08:00
Acknowledgments	<a href="#">Details</a>

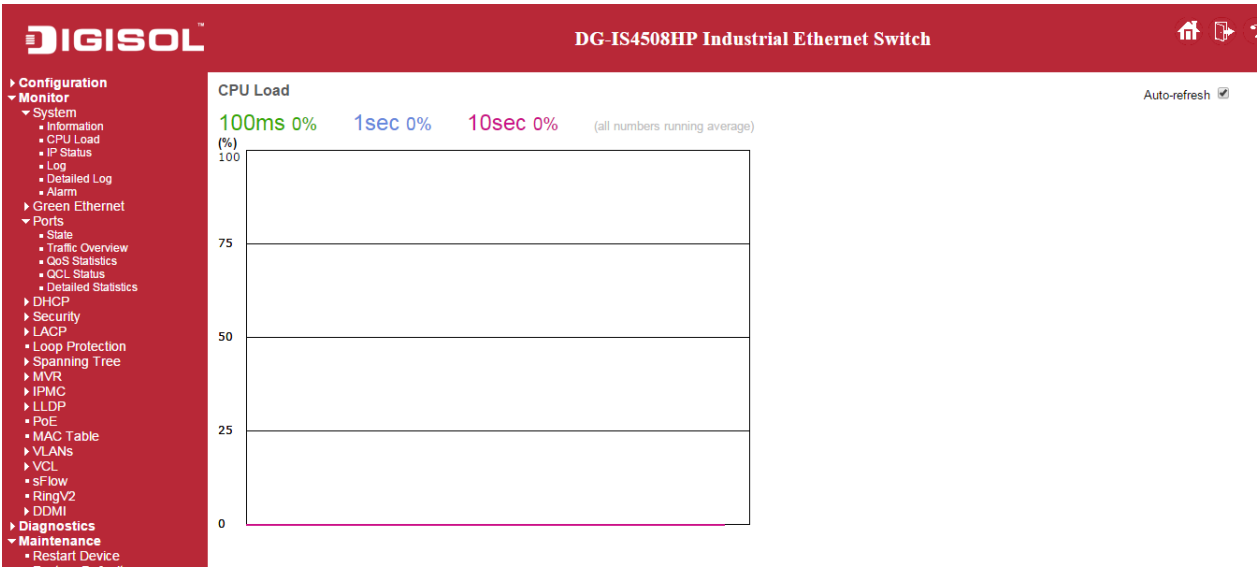
Object	Description
<b>Contact</b>	The system contact configured in Configuration   System   Information   System Contact.
<b>Name</b>	The system name configured in Configuration   System   Information   System Name.
<b>Location</b>	The system location configured in Configuration   System   Information   System Location.
<b>MAC Address</b>	The MAC Address of this switch.
<b>Chip ID</b>	The Chip ID of this switch.
<b>System Date</b>	The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.
<b>System Uptime</b>	The period of time the device has been operational.
<b>Software Version</b>	The software version of this switch.
<b>Software Date</b>	The date when the switch software was produced.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Click to refresh the page.

# CPU Load

This page displays the CPU load, using line chart.

The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 1~256 samples (maximum 256) are graphed, and the last numbers are displayed as text as well.



Buttons	
Auto-refresh <input checked="" type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

## IP Status

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbour cache (ARP cache) status.

**DIGISOL** DG-IS4508HP Industrial Ethernet Switch

Configuration Monitor

- System
  - Information
  - CPU Load
  - IP Status
  - Log
  - Detailed Log
  - Alarm
- Green Ethernet
- Ports
  - State
  - Traffic Overview
  - QoS Statistics
  - QoS Status
  - Detailed Statistics
- DHCP
- Security
- LACP
- Loop Protection
- Spanning Tree
- MVR
- IPMC
- LLDP
- PoE
- MAC Table
- VLANs
- VCL

Auto-refresh ☐ Refresh

### IP Interfaces

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	fe80::1::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	00-17-7c-6a-bd-72	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.0.2.1/24	
VLAN1	IPv6	fe80::2::217:7cff:fe6a:bd72/64	

### IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
192.0.2.0/24	VLAN1	<UP HW_RT>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

### Neighbour cache

IP Address	Link Address
192.0.2.90	VLAN1:14-fe-b5-bf-8d-d8
fe80::2::217:7cff:fe6a:bd72	VLAN1:00-17-7c-6a-bd-72

Object	Description
<b>IP Interfaces</b>	
<b>Interface</b>	The name of the interface.
<b>Type</b>	The address type of the entry. This may be <b>LINK</b> or <b>IPv4</b> .
<b>Address</b>	The current address of the interface (of the given type).
<b>Status</b>	The status flags of the interface (and/or address).
<b>IP Routes</b>	
<b>Network</b>	The destination IP network or host address of this route.
<b>Gateway</b>	The gateway address of this route.
<b>Status</b>	The status flags of the route.
<b>Neighbor cache</b>	
<b>IP Address</b>	The IP address of the entry.
<b>Link Address</b>	The Link (MAC) address for which a binding to the IP address given exist..

Buttons	
	Click to refresh the page.
<b>Auto-refresh</b> <input checked="" type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

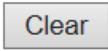


## System Log

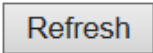
Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the web page will show the beginning entries of this table.

The "Level" input field is used to filter the display system log entries.

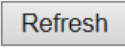
The "Clear Level" input field is used to specify which system log entries will be cleared.


To clear specific system log entries, select the clear level first then click the  button.


The "Start from ID" input field allow the user to change the starting point in this table. Clicking the

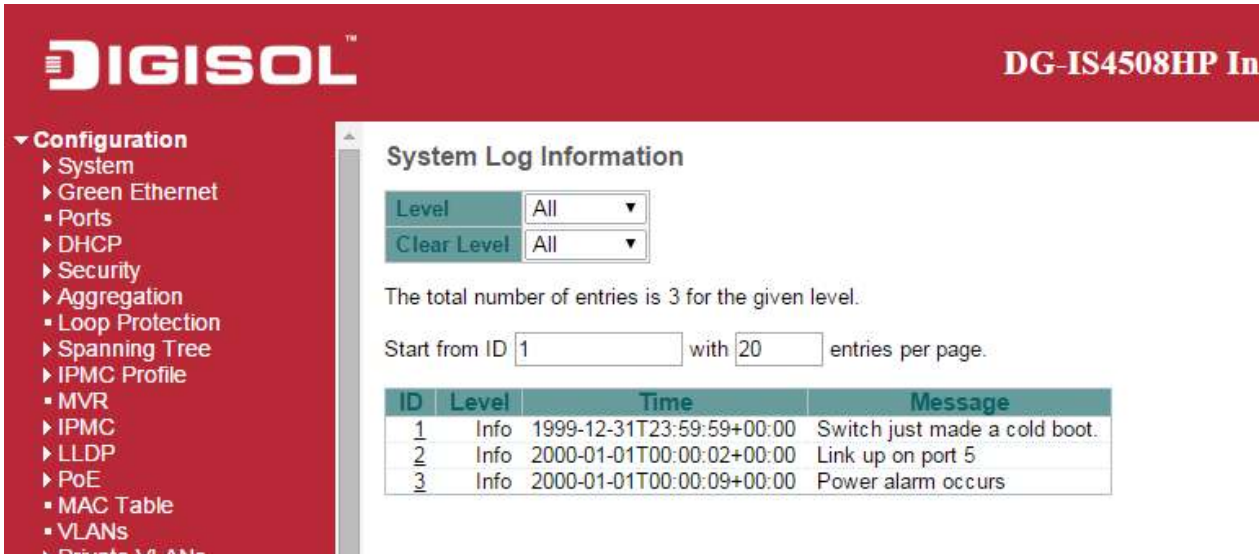


button will update the displayed table starting from that or the closest next entry match.

In addition, these input fields will upon a  button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

The  will use the last entry of the currently displayed table as a basis for the next lookup.

When the end is reached the text "No more entries" is shown in the displayed table. Use the  button to start over.



**DIGISOL** DG-IS4508HP In

▼ Configuration

- ▶ System
- ▶ Green Ethernet
- ▶ Ports
- ▶ DHCP
- ▶ Security
- ▶ Aggregation
- ▶ Loop Protection
- ▶ Spanning Tree
- ▶ IPMC Profile
- ▶ MVR
- ▶ IPMC
- ▶ LLDP
- ▶ PoE
- ▶ MAC Table
- ▶ VLANs
- ▶ Private VLANs

### System Log Information

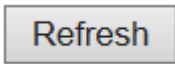
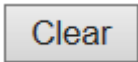
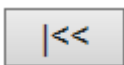
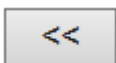

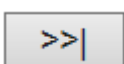
Level:  Clear Level:

The total number of entries is 3 for the given level.

Start from ID  with  entries per page.

ID	Level	Time	Message
1	Info	1999-12-31T23:59:59+00:00	Switch just made a cold boot.
2	Info	2000-01-01T00:00:02+00:00	Link up on port 5
3	Info	2000-01-01T00:00:09+00:00	Power alarm occurs

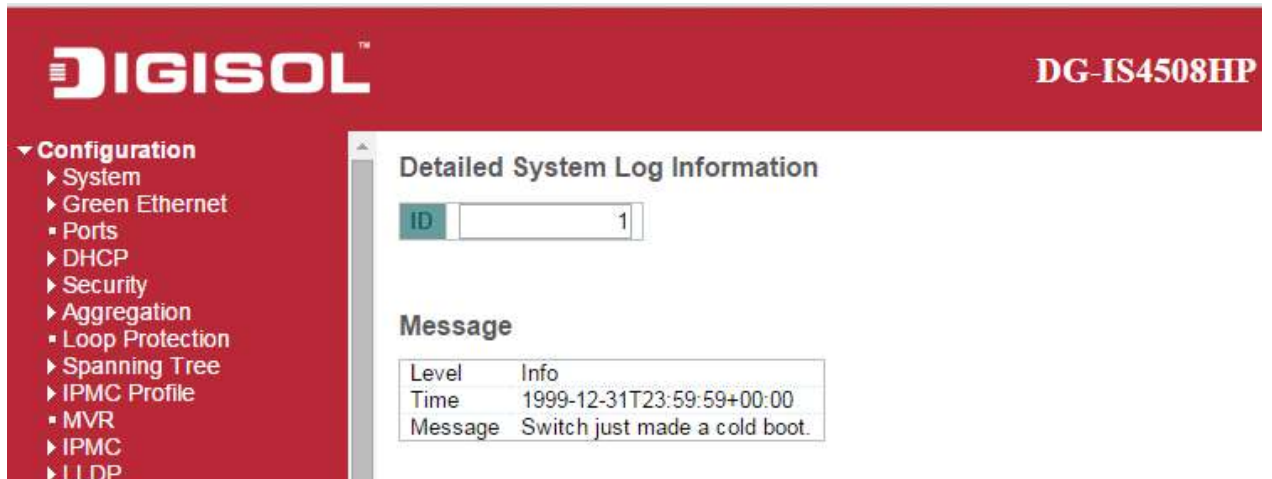
Object	Description
<b>ID</b>	The identification of the system log entry.
<b>Level</b>	The level of the system log entry. <b>Info</b> : The system log entry is belonged information level. <b>Warning</b> : The system log entry is belonged warning level. <b>Error</b> : The system log entry is belonged error level.
<b>Time</b>	The occurred time of the system log entry.
<b>Message</b>	The detail message of the system log entry.

Buttons	
Auto-refresh <input checked="" type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Updates the table entries, starting from the current entry.
	Flushes the selected entries.
	Updates the table entries, starting from the first available entry.
	Updates the table entries, ending at the last entry currently displayed.
	Updates the table entries, starting from the last entry currently displayed.
	Updates the table entries, ending at the last available entry.

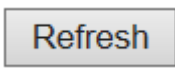
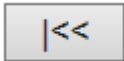
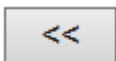

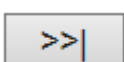


## System Detailed Log

The switch system detailed log information is provided here.



Object	Description
<b>ID</b>	The ID ( $\geq 1$ ) of the system log entry.
<b>Message</b>	The detailed message of the system log entry.

Buttons	
	Updates the system log entry to the current entry ID.
	Updates the system log entry to the first available entry ID.
	Updates the system log entry to the previous available entry ID.
	Updates the system log entry to the next available entry ID.
	Updates the system log entry to the last available entry ID.

# System Alarm

Current Alarm is provided on this page.



Object	Description
Description	Alarm Type Description..
Time	Alarm occurrence date time.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh data.

## Green Ethernet

### Port Power Saving

This page provides the current status for [EEE](#).

The screenshot shows the web interface of the DIGISOL DG-IS4508HP Industrial Ethernet Switch. The left sidebar contains a navigation menu with options like Configuration, Monitor, System, Green Ethernet, Port Power Savings, Ports, State, Traffic Overview, QoS Statistics, QoS Status, Detailed Statistics, DHCP, Security, LACP, Loop Protection, Spanning Tree, and MVR. The main content area displays the 'Port Power Savings Status' table. The table has columns for Port, Link, EEE, LP EEE Cap, EEE Savings, ActiPhy Savings, and PerfectReach Savings. The status for each port is indicated by a colored circle (green for up, red for down) and a checkmark or 'X' in the EEE column.

Port	Link	EEE	LP EEE Cap	EEE Savings	ActiPhy Savings	PerfectReach Savings
1	●	X	X	X	X	X
2	●	X	X	X	X	X
3	●	X	X	X	X	X
4	●	X	X	X	X	X
5	●	X	X	X	X	X
6	●	X	X	X	X	X
7	●	X	X	X	X	X
8	●	X	X	X	X	X

Object	Description
<b>Port</b>	This is the logical port number for this row.
<b>Link</b>	Shows if the link is up for the port (green = link up, red = link down).
<b>EEE</b>	Shows if <a href="#">EEE</a> is enabled for the port (reflects the settings at the Port Power Savings configuration page).
<b>LP EEE cap</b>	Shows if the link partner is <a href="#">EEE</a> capable.
<b>EEE Savings</b>	Shows if the system is currently saving power due to <a href="#">EEE</a> . When <a href="#">EEE</a> is enabled, the system will powered down if no frame has been received or transmitted in 5 uSec.
<b>ActiPhy Saving</b>	Shows if the system is currently saving power due to ActiPhy.
<b>PerfectReach Savings</b>	Shows if the system is currently saving power due to PerfectReach.

Buttons	
Auto-refresh <input checked="" type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page.

# Ports

## Ports State

This page provides an overview of the current switch port states.



The port states are illustrated as follows:

RJ45  
ports

SFP ports

State

Disabled

Down

Link

Buttons	
Auto-refresh <input checked="" type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
<div>Refresh</div>	Click to refresh the page.

## Traffic Overview

This page provides an overview of general traffic statistics for all switch ports.

DIGISOL™

DG-IS4508HP Industrial Ethernet Switch

Configuration

Monitor

System

Green Ethernet

- Port Power Savings

Ports

- State
- Traffic Overview
- QoS Statistics
- QCL Status
- Detailed Statistics

DHCP

Security

LACP

- Loop Protection

Port Statistics Overview

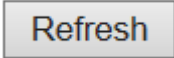
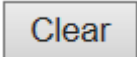
Auto-refresh

Refresh

Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	1560	1626	222592	288804	0	0	0	0	234
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0

Object	Description
<b>Port</b>	The logical port for the settings contained in the same row.
<b>Packet</b>	The number of received and transmitted packets per port.
<b>Bytes</b>	The number of received and transmitted bytes per port.
<b>Errors</b>	The number of frames received in error and the number of incomplete transmissions per port.
<b>Drops</b>	The number of frames discarded due to ingress or egress congestion.
<b>Filtered</b>	The number of received frames filtered by the forwarding process.

Buttons	
	Click to refresh the page immediately.
	Clears the counters for all ports.
Auto-refresh <input checked="" type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

## QoS Statistics

This page provides statistics for the different queues for all switch ports.

**DIGISOL™** DG-IS4508HP Industrial Ethernet Switch

Configuration  
Monitor  
System  
Green Ethernet  
Port Power Savings  
Ports  
State  
Traffic Overview  
QoS Statistics  
QoS Status  
Detailed Statistics  
DHCP  
Security  
LACP  
Loop Protection

Queuing Counters

Auto-refresh ☐ Refresh Clear

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	1571	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1654
6	0	0	0	0	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
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Object	Description
Port	The logical port for the settings contained in the same row.
Qn	There are 8 QoS queues per port. Q0 is the lowest priority queue.
Rx/Tx	The number of received and transmitted packets per queue

Buttons	
Auto-refresh <input checked="" type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page immediately.
Clear	Clears the counters for all ports.

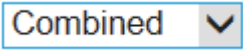
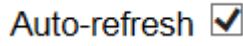

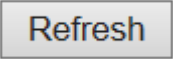
## QCL Status

This page shows the QCL status by different QCL users. Each row describes the [QCE](#) that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.



Object	Description
<b>User</b>	Indicates the QCL user.
<b>QCE</b>	Indicates the QCE id.
<b>Port</b>	Indicates the list of ports configured with the QCE.
<b>Frame Type</b>	Indicates the type of frame. Possible values are: <b>Any</b> : Match any frame type. <b>Ethernet</b> : Match Ethernet frames. <b>LLC</b> : Match ( <a href="#">LLC</a> ) frames. <b>SNAP</b> : Match ( <a href="#">SNAP</a> ) frames. <b>IPv4</b> : Match IPv4 frames. <b>IPv6</b> : Match IPv6 frames
<b>Action</b>	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are: <b>CoS</b> : Classify <a href="#">Class of Service</a> . <b>DPL</b> : Classify <a href="#">Drop Precedence Level</a> . <b>DSCP</b> : Classify <a href="#">DSCP</a> value.
<b>Conflict</b>	Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to

	add QCL entry on pressing 'Resolve Conflict' button.
--	--

Buttons	
	Select the QCL status from this drop down list.
	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.
	Click to refresh the page.



## Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

DIGISOL™

Configuration

Monitor

- System
- Green Ethernet
  - Port Power Savings
- Ports
  - State
  - Traffic Overview
  - QoS Statistics
  - QCL Status
  - Detailed Statistics
- DHCP
- Security
- LACP
- Loop Protection
- Spanning Tree
- MVR
- IPMC
- LLDP
- PoE
- MAC Table
- VLANs
- VCL
- sFlow
- RingV2
- DDMI

- Diagnostics
- Maintenance
- Restart Device
- Factory Defaults
- Software
- Configuration

DG-IS4508HP Industrial Ethernet Switch

Port 1

Auto-refresh

Refresh

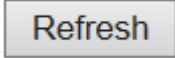
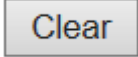
Clear

Detailed Port Statistics Port 1

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	0
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

Object	Description
<b>Receive Total and Transmit Total</b>	
<b>Rx and Tx Packets</b>	The number of received and transmitted (good and bad) packets.
<b>Rx and Tx Octets</b>	The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
<b>Rx and Tx Unicast</b>	The number of received and transmitted (good and bad) unicast packets.
<b>Rx and Tx Multicast</b>	The number of received and transmitted (good and bad) multicast packets.
<b>Rx and Tx Broadcast</b>	The number of received and transmitted (good and bad) broadcast packets.
<b>Rx and Tx Pause</b>	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
<b>Receive and Transmit Size Counters</b>	

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.	
<b>Receive and Transmit Queue Counters</b>	
The number of received and transmitted packets per input and output queue.	
<b>Receive Error Counters</b>	
<b>Rx Drops</b>	The number of frames dropped due to lack of receive buffers or egress congestion.
<b>Rx CRC/Alignment</b>	The number of frames received with CRC or alignment errors.
<b>Rx Undersize</b>	The number of short <sup>1</sup> frames received with valid CRC.
<b>Rx Oversize</b>	The number of long <sup>2</sup> frames received with valid CRC.
<b>Rx Fragments</b>	The number of short <sup>1</sup> frames received with invalid CRC.
<b>Rx Jabber</b>	The number of long <sup>2</sup> frames received with invalid CRC.
<b>Rx Filtered</b>	<p>The number of received frames filtered by the forwarding process.</p> <p><sup>1</sup> Short frames are frames that are smaller than 64 bytes.</p> <p><sup>2</sup> Long frames are frames that are longer than the configured maximum frame length for this port.</p>
<b>Transmit Error Counters</b>	
<b>Tx Drops</b>	The number of frames dropped due to output buffer congestion.
<b>Tx Late/Exc. Coll</b>	The number of frames dropped due to excessive or late collisions.

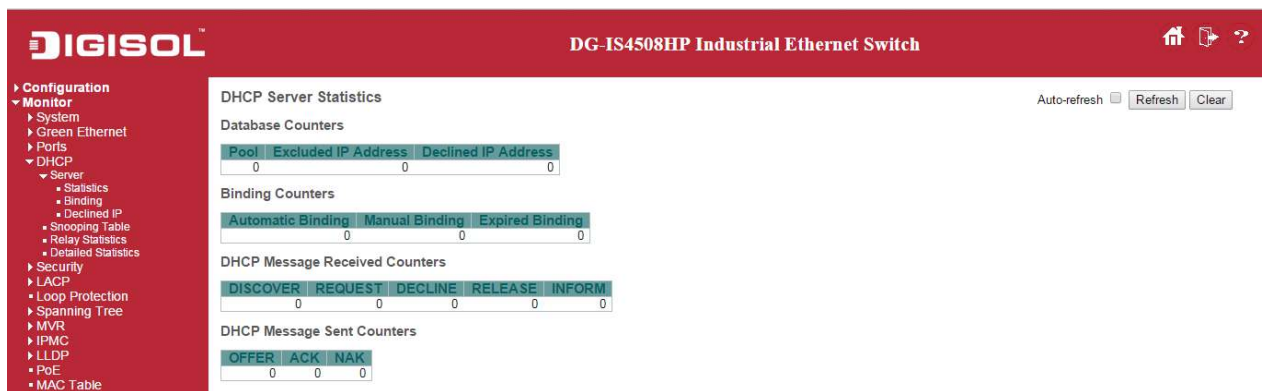
Buttons	
	Click to refresh the page immediately.
	Click to refresh the page immediately.
<b>Auto-refresh</b> <input checked="" type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

# DHCP

## DHCP Server

### Statistics

This page displays the database counters and the number of DHCP messages sent and received by DHCP server.



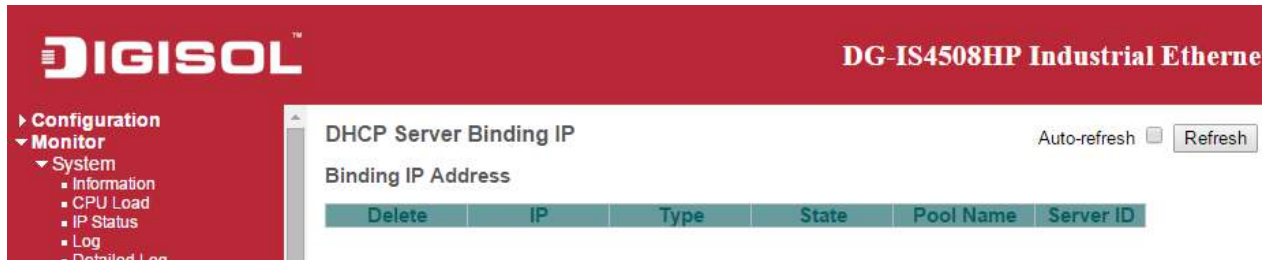
Object	Description
<b>Database Counters</b>	
<b>Pool</b>	Number of pools.
<b>Excluded IP Address</b>	Number of excluded IP address ranges.
<b>Declined IP Address</b>	Number of declined IP addresses.
<b>Binding Counters</b>	
<b>Automatic Binding</b>	Number of bindings with network-type pools.
<b>Manual Binding</b>	Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type.
<b>Expired Binding</b>	Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings.
<b>DHCP Message Received Counters</b>	
<b>DISCOVER</b>	Number of DHCP DISCOVER messages received.
<b>REQUEST</b>	Number of DHCP REQUEST messages received.
<b>DECLINE</b>	Number of DHCP DECLINE messages received.
<b>RELEASE</b>	Number of DHCP RELEASE messages received.

<b>INFORM</b>	Number of DHCP INFORM messages received.
<b>DHCP Message Sent Counters</b>	
<b>OFFER</b>	Number of DHCP OFFER messages sent.
<b>ACK</b>	Number of DHCP ACK messages sent.
<b>NAK</b>	Number of DHCP NAK messages sent.

<b>Buttons</b>	
Auto-refresh <input checked="" type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.
<input type="button" value="Clear"/>	Click to Clears DHCP Message Received Counters and DHCP Message Sent Counters.

## Binding

This page displays bindings generated for DHCP clients.



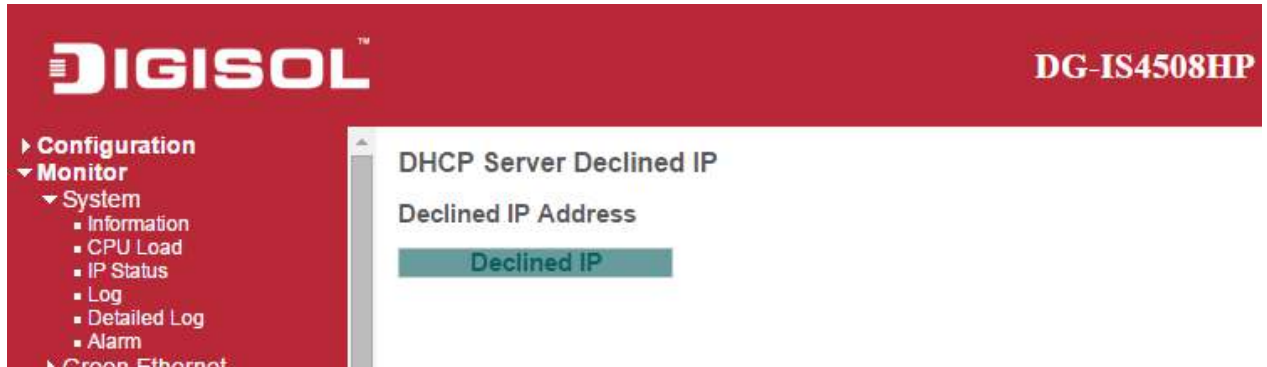
Object	Description
IP	IP address allocated to DHCP client.
Type	Type of binding. Possible types are Automatic, Manual, Expired.
State	State of binding. Possible states are Committed, Allocated, Expired.
Pool Name	The pool that generates the binding.
Server ID	Server IP address to service the binding.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page immediately.
Clear Selected	Click to clear selected bindings. If the selected binding is Automatic or Manual, then it is changed to be Expired. If the selected binding is Expired, then it is freed.
Clear Automatic	Click to clear all Automatic bindings and Change them to Expired bindings.
Clear Manual	Click to clear all Manual bindings and Change them to Expired bindings.
Clear Expired	Click to clear all Expired bindings and free them.



## Declined IP

This page displays declined IP addresses.



Object	Description
Declined IP	List of IP addresses declined.

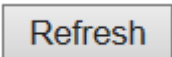
Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.

## DHCP Snooping Table

Each page shows up to 99 entries from the Dynamic DHCP snooping table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic DHCP snooping Table.

The "MAC address" and "VLAN" input fields allows the user to select the starting point in the Dynamic

DHCP snooping Table. Clicking the  button will update the displayed table starting from that or the closest next Dynamic DHCP snooping Table match. In addition, the two input fields will -

upon a  button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The  will use the last entry of the currently displayed table as a basis for the next lookup.

When the end is reached the text "No more entries" is shown in the displayed table. Use the


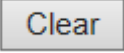
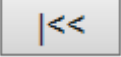

 button to start over.



Object	Description
<b>MAC Address</b>	User MAC address of the entry.
<b>VLAN ID</b>	VLAN-ID in which the DHCP traffic is permitted.
<b>Source Port</b>	Switch Port Number for which the entries are displayed.
<b>IP Address</b>	User IP address of the entry.
<b>IP Subnet Mask</b>	User IP subnet mask of the entry.
<b>DHCP Server Address</b>	DHCP Server address of the entry.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.



	Refreshes the displayed table starting from the input fields.
	Flushes all dynamic entries.
	Updates the table starting from the first entry in the Dynamic DHCP snooping Table.
	Updates the table, starting with the entry after the last entry currently displayed.

## DHCP Relay Statistics

This page provides statistics for [DHCP relay](#).



Object	Description
<b>Server Statistics</b>	
<b>Transmit to Server</b>	The number of packets that are relayed from client to server.
<b>Transmit Error</b>	The number of packets that resulted in errors while being sent to clients.
<b>Receive from Server</b>	The number of packets received from server.
<b>Receive Missing Agent Option</b>	The number of packets received without agent information options.
<b>Receive Missing Circuit ID</b>	The number of packets received with the Circuit ID option missing.
<b>Receive Missing Remote ID</b>	The number of packets received with the Remote ID option missing.
<b>Receive Bad Circuit ID</b>	The number of packets whose Circuit ID option did not match known circuit ID.
<b>Receive Bad Remote ID</b>	The number of packets whose Remote ID option did not match known Remote ID.
<b>Client Statistics</b>	
<b>Transmit to Client</b>	The number of relayed packets from server to client.
<b>Transmit Error</b>	The number of packets that resulted in error while being sent to servers.
<b>Receive from Client</b>	The number of received packets from server.
<b>Receive Agent Option</b>	The number of received packets with relay agent information option.
<b>Replace Agent Option</b>	The number of packets which were replaced with relay agent information option.
<b>Keep Agent Option</b>	The number of packets whose relay agent information was retained.
<b>Drop Agent Option</b>	The number of packets that were dropped which were received with relay agent information.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.
<input type="button" value="Clear"/>	Clear all statistics.

## DHCP Detailed Statistics

This page provides statistics for [DHCP snooping](#). Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism. And clear the statistics on specific port may not take effect on global statistics since it gathers the different layer overview.

**DIGISOL** DG-IS4508HP Industrial Ethernet Switch

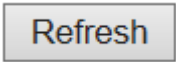
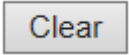
Configuration  
Monitor  
System  
Green Ethernet  
Ports  
DHCP  
Server  
Statistics  
Binding  
Declined IP  
Snooping Table  
Relay Statistics  
Detailed Statistics  
Security  
Access Management  
Statistics  
Network  
AAA  
Switch  
LACP

DHCP Detailed Statistics Port 1

Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0
Rx Discarded Checksum Error	0		
Rx Discarded from Untrusted	0		

Object	Description
<b>Rx and Tx Discover</b>	The number of discover (option 53 with value 1) packets received and transmitted.
<b>Rx and Tx Offer</b>	The number of offer (option 53 with value 2) packets received and transmitted.
<b>Rx and Tx Request</b>	The number of request (option 53 with value 3) packets received and transmitted.
<b>Rx and Tx Decline</b>	The number of decline (option 53 with value 4) packets received and transmitted.
<b>Rx and Tx ACK</b>	The number of ACK (option 53 with value 5) packets received and transmitted.
<b>Rx and Tx NAK</b>	The number of NAK (option 53 with value 6) packets received and transmitted.
<b>Rx and Tx Release</b>	The number of release (option 53 with value 7) packets received and transmitted.
<b>Rx and Tx Inform</b>	The number of inform (option 53 with value 8) packets received and transmitted.
<b>Rx and Tx Lease Query</b>	The number of lease query (option 53 with value 10) packets received and transmitted.
<b>Rx and Tx Lease Unassigned</b>	The number of lease unassigned (option 53 with value 11) packets received and transmitted.
<b>Rx and Tx Unknown</b>	The number of lease unknown (option 53 with value 12) packets received and transmitted.
<b>Rx and Tx Active</b>	The number of lease active (option 53 with value 13) packets received and transmitted.
<b>Rx Discarded checksum</b>	The number of discard packet that IP/UDP checksum is error.

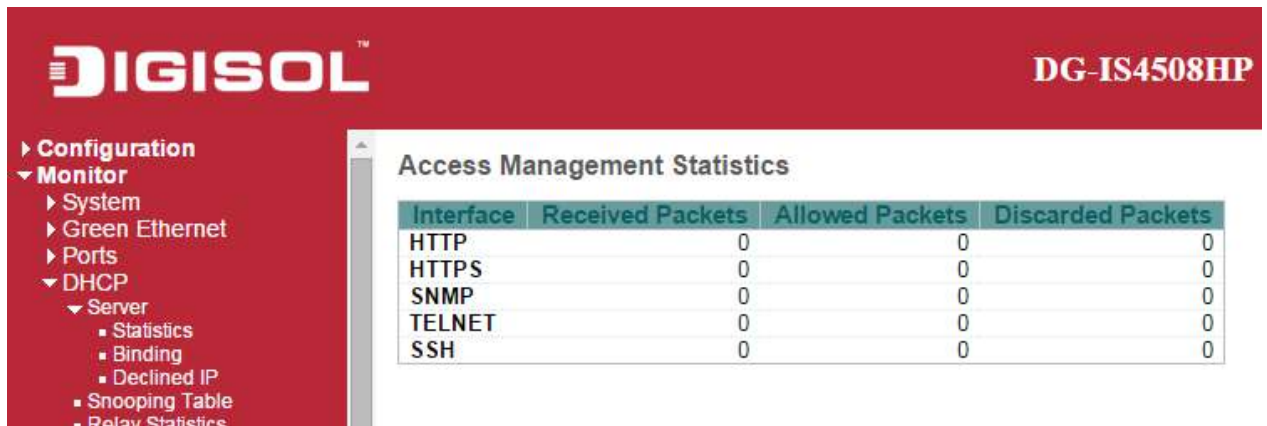
<b>error</b>	
<b>Rx Discarded from Untrusted</b>	The number of discarded packet that are coming from untrusted port.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Refreshes the displayed table starting from the input fields.
	Flushes all dynamic entries.

## Security

### Accessment Management Statistics

This page provides statistics for access management.



**DIGISOL™** **DG-IS4508HP**

► Configuration  
▼ Monitor  
  ► System  
  ► Green Ethernet  
  ► Ports  
  ▼ DHCP  
    ▼ Server  
      ■ Statistics  
      ■ Binding  
      ■ Declined IP  
      ■ Snooping Table  
      ■ Relay Statistics

#### Access Management Statistics

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

Object	Description
<b>Interface</b>	The interface type through which the remote host can access the switch.
<b>Received Packets</b>	Number of received packets from the interface when access management mode is enabled.
<b>Allowed Packets</b>	Number of allowed packets from the interface when access management mode is enabled.
<b>Discarded Packets</b>	Number of discarded packets from the interface when access management mode is enabled.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.
<input type="button" value="Clear"/>	Clear all statistics.

## Network

## Port Security

## Switch

This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

**DIGISOL** DG-IS4508HP

- Configuration
- ▼ Monitor
  - System
  - Green Ethernet
  - Ports
  - ▼ DHCP
    - ▼ Server
      - Statistics
      - Binding
      - Declined IP
      - Snooping Table
      - Relay Statistics
      - Detailed Statistics
  - ▼ Security
    - Access Management
    - Statistics
    - ▼ Network
      - ▼ Port Security
        - Switch
        - Port
      - NAS
      - ACL Status
      - ARP Inspection
      - IP Source Guard
    - AAA

**Port Security Switch Status**

**User Module Legend**

User Module Name	Abbr
Limit Control	L
802.1X	8
DHCP Snooping	D
Voice VLAN	V

**Port Status**

Port	Users	State	MAC Count	
			Current	Limit
1	----	Disabled	-	-
2	----	Disabled	-	-
3	----	Disabled	-	-
4	----	Disabled	-	-
5	----	Disabled	-	-
6	----	Disabled	-	-
7	----	Disabled	-	-
8	----	Disabled	-	-

Object	Description
<a href="#">User Module Legend</a>	

<b>User Module Name</b>	The full name of a module that may request Port Security services.
<b>Abbr</b>	A one-letter abbreviation of the user module. This is used in the <a href="#">Users</a> column in the port status table.
<b>Port Status</b>	
<b>Port</b>	The port number for which the status applies. Click the port number to see the status for this particular port.
<b>Users</b>	Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see <a href="#">Abbr</a> ) has enabled port security.
<b>State</b>	Shows the current state of the port. It can take one of four values: <b>Disabled:</b> No user modules are currently using the Port Security service. <b>Ready:</b> The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive. <b>Limit Reached:</b> The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in. <b>Shutdown:</b> The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.
<b>MAC Count (Current, Limit)</b>	The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.  If no user modules are enabled on the port, the Current column will show a dash (-).  If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

<b>Buttons</b>	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds
<input type="button" value="Refresh"/>	Click to refresh the page immediately.





## Port

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.



Object	Description
<b>MAC Address &amp; VLAN ID</b>	The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating <i>"No MAC addresses attached"</i> is displayed.
<b>State</b>	Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.
<b>Time of Addition</b>	Shows the date and time when this MAC address was first seen on the port.
<b>Age/Hold</b>	<p>If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.</p> <p>If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.</p>

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.

# NAS

## Switch

This page provides an overview of the current [NAS](#) port states.

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
3	Force Authorized	Globally Disabled			-	
4	Force Authorized	Globally Disabled			-	
5	Force Authorized	Globally Disabled			-	
6	Force Authorized	Globally Disabled			-	
7	Force Authorized	Globally Disabled			-	
8	Force Authorized	Globally Disabled			-	

Object	Description
<b>Port</b>	The switch port number. Click to navigate to detailed NAS statistics for this port.
<b>Admin State</b>	The port's current administrative state. Refer to NAS <a href="#">Admin State</a> for a description of possible values.
<b>Port State</b>	The current state of the port. Refer to NAS <a href="#">Port State</a> for a description of the individual states.
<b>Last Source</b>	The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.
<b>Last ID</b>	The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.
<b>QoS Class</b>	QoS Class assigned to the port by the RADIUS server if enabled.
<b>Port VLAN ID</b>	<p>The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.</p> <p>If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs <a href="#">here</a>.</p> <p>If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read</p>

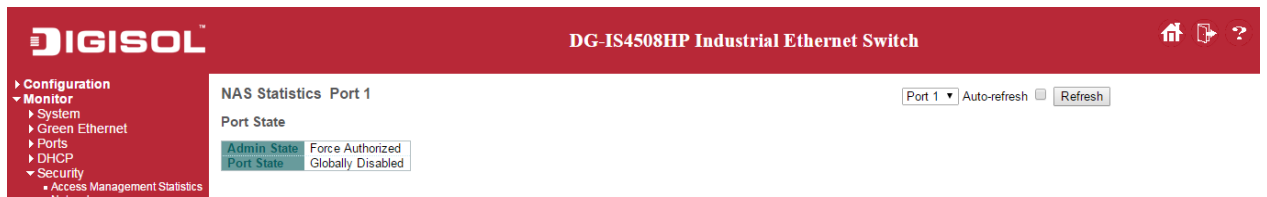
	more about Guest VLANs <a href="#">here</a> .
--	---

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.

## Port

This page provides detailed [NAS](#) statistics for a specific switch port running EAPOL-based [IEEE 802.1X](#) authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only .


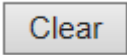
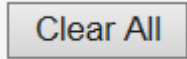
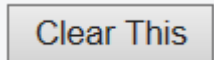
Use the port select box to select which port details to be displayed.



Object	Description
<b>Port State</b>	
<b>Admin State</b>	The port's current administrative state. Refer to NAS <a href="#">Admin State</a> for a description of possible values.
<b>Port State</b>	The current state of the port. Refer to NAS <a href="#">Port State</a> for a description of the individual states.
<b>QoS Class</b>	The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.
<b>Port VLAN ID</b>	<p>The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.</p> <p>If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs <a href="#">here</a>.</p> <p>If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs <a href="#">here</a>.</p>
<b>Port Counters</b>	
<b>EAPOL Counters</b>	<p>These supplicant frame counters are available for the following <a href="#">administrative states</a>:</p> <ul style="list-style-type: none"> <li>• Force Authorized</li> <li>• Force Unauthorized</li> <li>• Port-based 802.1X</li> <li>• Single 802.1X</li> <li>• Multi 802.1X</li> </ul>
<b>Backend Server</b>	These backend (RADIUS) frame counters are available for the following

<b>Counters</b>	<a href="#">administrative states</a> : <ul style="list-style-type: none"> <li>• Port-based 802.1X</li> <li>• Single 802.1X</li> <li>• Multi 802.1X</li> <li>• MAC-based Auth.</li> </ul>
<b>Last Supplicant/Client Info</b>	<p>Information about the last supplicant/client that attempted to authenticate. This information is available for the following <a href="#">administrative states</a>:</p> <ul style="list-style-type: none"> <li>• Port-based 802.1X</li> <li>• Single 802.1X</li> <li>• Multi 802.1X</li> <li>• MAC-based Auth.</li> </ul>
<b>Selected Counters</b>	
<b>Selected Counters</b>	<p>The Selected Counters table is visible when the port is in one of the following <a href="#">administrative states</a>:</p> <ul style="list-style-type: none"> <li>• Multi 802.1X</li> <li>• MAC-based Auth.</li> </ul> <p>The table is identical to and is placed next to the <a href="#">Port Counters</a> table, and will be empty if no MAC address is currently selected. To populate the table, select one of the <a href="#">attached MAC Addresses</a> from the table below.</p>
<b>Attached MAC Addresses</b>	
<b>Identity</b>	<p>Shows the identity of the supplicant, as received in the Response Identity EAPOL frame.</p> <p>Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows <i>No supplicants attached</i>.</p> <p>This column is not available for MAC-based Auth.</p>
<b>MAC Address</b>	<p>For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based Auth., this column holds the MAC address of the attached client.</p> <p>Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows <i>No clients attached</i>.</p>
<b>VLAN ID</b>	<p>This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.</p>
<b>State</b>	<p>The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it</p>

	is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for <a href="#">Hold Time</a> seconds.
<b>Last Authentication</b>	Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Click to refresh the page immediat
	<p>This button is available in the following modes:</p> <ul style="list-style-type: none"> <li>• Force Authorized</li> <li>• Force Unauthorized</li> <li>• Port-based 802.1X</li> <li>• Single 802.1X</li> </ul> <p>Click to clear the counters for the selected port.</p>
	<p>This button is available in the following modes:</p> <ul style="list-style-type: none"> <li>• Multi 802.1X</li> <li>• MAC-based Auth.X</li> </ul> <p>Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however.</p>
	<p>This button is available in the following modes:</p> <ul style="list-style-type: none"> <li>• Multi 802.1X</li> <li>• MAC-based Auth.X</li> </ul> <p>Click to clear only the currently selected client's counters.</p>



## ACL Status

This page shows the ACL status by different ACL users. Each row describes the [ACE](#) that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is **256** on each switch.

DIGISOL™ DG-IS4508HP Industrial Ethernet Switch										
Configuration Monitor System Green Ethernet Ports DHCP Security Access Management Statistics	ACL Status									
	User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter
	LLDP	All	EType-0x88cc	Deny	Disabled	Disabled	Disabled	Yes	No	0 No
	RING	All	EType	Deny	Disabled	Disabled	Disabled	Yes	No	0 No
	Conflict									

Object	Description
<b>User</b>	Indicates the ACL user.
<b>Ingress Port</b>	Indicates the ingress port of the ACE. Possible values are: <b>All</b> : The ACE will match all ingress port. <b>Port</b> : The ACE will match a specific ingress port.
<b>Frame Type</b>	Indicates the frame type of the ACE. Possible values are: <b>Any</b> : The ACE will match any frame type. <b>EType</b> : The ACE will match <a href="#">Ethernet Type</a> frames. Note that an Ethernet Type based ACE will not get matched by <a href="#">IP</a> and <a href="#">ARP</a> frames. <b>ARP</b> : The ACE will match ARP/ <a href="#">RARP</a> frames. <b>IPv4</b> : The ACE will match all IPv4 frames. <b>IPv4/ICMP</b> : The ACE will match IPv4 frames with ICMP protocol. <b>IPv4/UDP</b> : The ACE will match IPv4 frames with UDP protocol. <b>IPv4/TCP</b> : The ACE will match IPv4 frames with TCP protocol. <b>IPv4/Other</b> : The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. <b>IPv6</b> : The ACE will match all IPv6 standard frames.
<b>Action</b>	Indicates the forwarding action of the ACE. <b>Permit</b> : Frames matching the ACE may be forwarded and learned. <b>Deny</b> : Frames matching the ACE are dropped. <b>Filter</b> : Frames matching the ACE are filtered.
<b>Rate limiter</b>	Indicates the rate limiter number of the ACE. The allowed range is <b>1</b> to <b>16</b> . When <b>Disabled</b> is displayed, the rate limiter operation is disabled.
<b>Port Redirect</b>	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are <b>Disabled</b> or a specific port

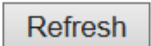
	number. When <b>Disabled</b> is displayed, the port redirect operation is disabled.
<b>Mirror</b>	Specify the mirror operation of this port. The allowed values are: <b>Enabled</b> : Frames received on the port are mirrored. <b>Disabled</b> : Frames received on the port are not mirrored. The default value is "Disabled".
<b>CPU</b>	Forward packet that matched the specific ACE to CPU.
<b>CPU Once</b>	Forward first packet that matched the specific ACE to CPU.
<b>Counter</b>	The counter indicates the number of times the ACE was hit by a frame.
<b>Conflict</b>	Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.


Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds..
<input type="button" value="Refresh"/>	Click to refresh the page.

## ARP Inspection


Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

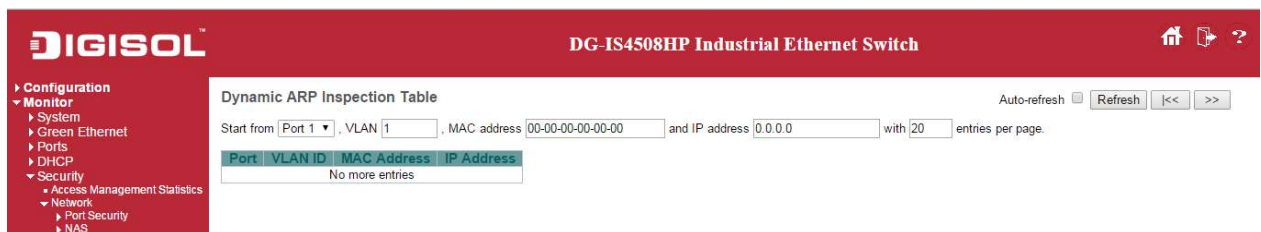
The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to

select the starting point in the Dynamic ARP Inspection Table. Clicking the  button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match.

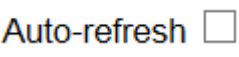
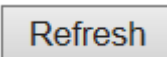
In addition, the two input fields will - upon a  button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

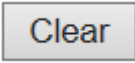
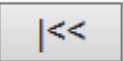

The  will use the last entry of the currently displayed table as a basis for the next lookup.

When the end is reached the text "No more entries" is shown in the displayed table. Use the  button to start over.



Object	Description
<b>Port</b>	Switch Port Number for which the entries are displayed.
<b>VLAN ID</b>	VLAN-ID in which the ARP traffic is permitted.
<b>MAC Address</b>	User MAC address of the entry.
<b>IP Address</b>	User IP address of the entry.


Buttons	
	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Refreshes the displayed table starting from the input fields.


	<p>Flushes all dynamic entries.</p>
	<p>Updates the table starting from the first entry in the Dynamic ARP Inspection Table.</p>
	<p>Updates the table, starting with the entry after the last entry currently displayed.</p>


## IP Source Guard

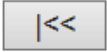
Each page shows up to 99 entries from the Dynamic IP Source Guard table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic IP Source Guard Table.

The "Start from port address", "VLAN" and "IP address" input fields allow the user to select the starting

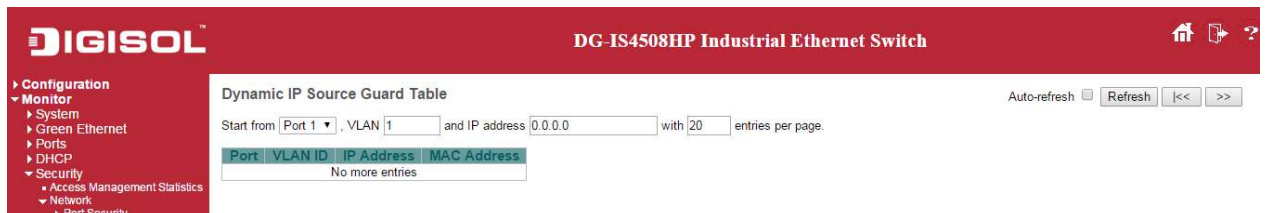
point in the Dynamic IP Source Guard Table. Clicking the  button will update the displayed table starting from that or the closest next Dynamic IP Source Guard Table match. In

addition, the two input fields will - upon a  button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

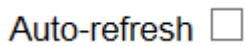
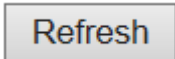
The  will use the last entry of the currently displayed table as a basis for the next lookup.

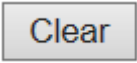
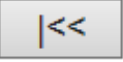

When the end is reached the text "No more entries" is shown in the displayed table. Use the 

button to start over.



Object	Description
<b>Port</b>	Switch Port Number for which the entries are displayed.
<b>VLAN ID</b>	VLAN-ID in which the IP traffic is permitted.
<b>IP Address</b>	User IP address of the entry.
<b>MAC Address</b>	Source MAC address.

Buttons	
	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Refresh the displayed table starting from the input fields.

	Flush all dynamic entries.
	Update the table starting from the first entry in the Dynamic IP Source Guard Table.
	Updates the table, starting with the entry after the last entry currently displayed.

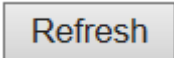
# AAA

## RADIUS Overview

This page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page.

Object	Description
<b>RADIUS Authentication Servers</b>	
<b>#</b>	The RADIUS server number. Click to navigate to detailed statistics for this server.
<b>IP Address</b>	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
<b>Status</b>	<p>The current status of the server. This field takes one of the following values:</p> <p><b>Disabled:</b> The server is disabled.</p> <p><b>Not Ready:</b> The server is enabled, but IP communication is not yet up and running.</p> <p><b>Ready:</b> The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.</p> <p><b>Dead (X seconds left):</b> Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.</p>
<b>RADIUS Accounting Servers</b>	
<b>#</b>	The RADIUS server number. Click to navigate to detailed statistics for this server.
<b>IP Address</b>	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

<b>Status</b>	<p>The current status of the server. This field takes one of the following values:</p> <p><b>Disabled:</b> The server is disabled.</p> <p><b>Not Ready:</b> The server is enabled, but IP communication is not yet up and running.</p> <p><b>Ready:</b> The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.</p> <p><b>Dead (X seconds left):</b> Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.</p>
---------------	---

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Click to refresh the page immediately.



## RADIUS Details

This page provides detailed statistics for a particular RADIUS server.

The screenshot shows the DIGISOL web interface for the DG-IS4508HP Industrial Ethernet Switch. The left sidebar contains a navigation menu with options like Configuration, Monitor, System, Green Ethernet, Ports, DHCP, Security, Access Management Statistics, Network, AAA, RADIUS Overview, RADIUS Details, Switch, LACP, Loop Protection, Spanning Tree, MVR, IPMC, LLDP, PoE, MAC Table, VLANs, VCL, sFlow, RingV2, DDM, Diagnostics, and Maintenance. The main content area displays 'RADIUS Authentication Statistics for Server #1' and 'RADIUS Accounting Statistics for Server #1'. Each section includes a table of packet counters (Receive and Transmit) and other information like IP Address, State, and Round-Trip Time.

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		

Object	Description
<b>RADIUS Authentication Statistics</b>	
<b>Packet Counters</b>	RADIUS authentication server packet counter. There are seven receive and four transmit counters.
<b>Other Info</b>	This section contains information about the state of the server and the latest round-trip time.
<b>RADIUS Accounting Statistics</b>	
<b>Packet Counters</b>	RADIUS accounting server packet counter. There are five receive and four transmit counters.
<b>Other Info</b>	This section contains information about the state of the server and the latest round-trip time.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.

<div data-bbox="272 259 408 315" style="border: 1px solid black; padding: 2px 10px; display: inline-block;">Clear</div>	Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.
---	--

## Switch

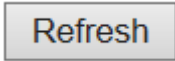
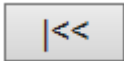
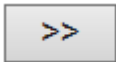
## RMON

## Statistics

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

Object	Description
<b>ID</b>	Indicates the index of Statistics entry.
<b>Data Source(ifIndex)</b>	The port ID which wants to be monitored.
<b>Drop</b>	The total number of events in which packets were dropped by the probe due to lack of resources.
<b>Octets</b>	The total number of octets of data (including those in bad packets) received on the network.
<b>Pkts</b>	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
<b>Broad-cast</b>	The total number of good packets received that were directed to the broadcast address.
<b>Multi-cast</b>	The total number of good packets received that were directed to a multicast address.
<b>CRC Errors</b>	The total number of packets received that had a length (excluding framing bits, but

	including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
<b>Under-Size</b>	The total number of packets received that were less than 64 octets.
<b>Over-size</b>	The total number of packets received that were longer than 1518 octets.
<b>Frag.</b>	The number of frames which size is less than 64 octets received with invalid CRC.
<b>Jabb.</b>	The number of frames which size is larger than 64 octets received with invalid CRC.
<b>Coll.</b>	The best estimate of the total number of collisions on this Ethernet segment.
<b>64</b>	The total number of packets (including bad packets) received that were 64 octets in length.
<b>65~127</b>	The total number of packets (including bad packets) received that were between 65 to 127 octets in length.
<b>128~255</b>	The total number of packets (including bad packets) received that were between 128 to 255 octets in length.
<b>256~511</b>	The total number of packets (including bad packets) received that were between 256 to 511 octets in length.
<b>512~1023</b>	The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.
<b>1024~1588</b>	The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.


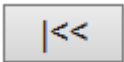
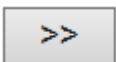
Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Click to refresh the page immediately.
	Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.
	Updates the table, starting with the entry after the last entry currently displayed.

## History

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.

Object	Description
<b>History Index</b>	Indicates the index of History control entry.
<b>Sample Index</b>	Indicates the index of the data entry associated with the control entry.
<b>Sample Start</b>	The value of sysUpTime at the start of the interval over which this sample was measured.
<b>Drop</b>	The total number of events in which packets were dropped by the probe due to lack of resources.
<b>Octets</b>	The total number of octets of data (including those in bad packets) received on the network.
<b>Pkts</b>	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
<b>Broadcast</b>	The total number of good packets received that were directed to the broadcast address.
<b>Multicast</b>	The total number of good packets received that were directed to a multicast address.
<b>CRC Errors</b>	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
<b>Undersize</b>	The total number of packets received that were less than 64 octets.
<b>Oversize</b>	The total number of packets received that were longer than 1518 octets.
<b>Frag.</b>	The number of frames which size is less than 64 octets received with invalid CRC.
<b>Jabb.</b>	The number of frames which size is larger than 64 octets received with invalid CRC.

<b>Coll.</b>	The best estimate of the total number of collisions on this Ethernet segment.
<b>Utilization</b>	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Click to refresh the page immediately.
	Updates the table starting from the first entry in the History table, i.e., the entry with the lowest History Index and Sample Index.
	Updates the table, starting with the entry after the last entry currently displayed.

## Alarm

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.

**DIGISOL** DG-IS4508HP Industrial Ethernet

Configuration  
Monitor  
System  
Green Ethernet  
Ports  
DHCP  
Server  
Statistics  
Binding  
Declined IP  
Snooping Table  
Relay Statistics


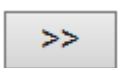
**RMON Alarm Overview**

Start from Control Index  with  entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No more entries									

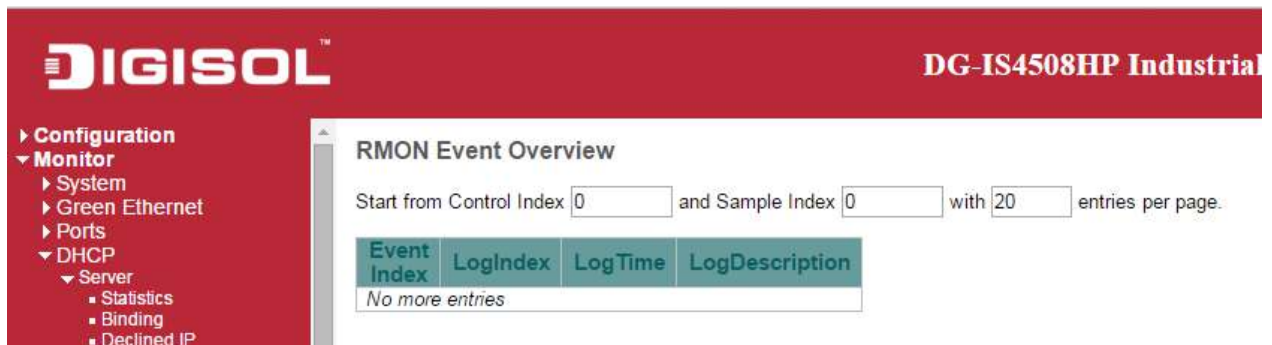
Object	Description
<b>ID</b>	Indicates the index of Alarm control entry.
<b>Interval</b>	Indicates the interval in seconds for sampling and comparing the rising and falling threshold.
<b>Variable</b>	Indicates the particular variable to be sampled.
<b>Sample Type</b>	The method of sampling the selected variable and calculating the value to be compared against the thresholds.
<b>Value</b>	The value of the statistic during the last sampling period.
<b>Startup Alarm</b>	The alarm that may be sent when this entry is first set to valid.
<b>Rising Threshold</b>	Rising threshold value.
<b>Rising Index</b>	Rising event index.
<b>Falling Threshold</b>	Falling threshold value.
<b>Falling Index</b>	Falling event index.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.

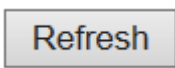
	Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.
	Updates the table, starting with the entry after the last entry currently displayed.

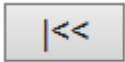

## Event

This page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table.



Object	Description
<b>Event Index</b>	Indicates the index of the event entry.
<b>Log Index</b>	Indicates the index of the log entry.
<b>Log Time</b>	Indicates Event log time.
<b>LogDescription</b>	Indicates the Event description.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Click to refresh the page immediately.

	<p>Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index.</p>
	<p>Updates the table, starting with the entry after the last entry currently displayed.</p>



# LACP

## System Status

This page provides a status overview for all [LACP](#) instances.

**DIGISOL™** DG-IS4508HP Industrial Ethernet Switch

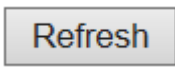
Configuration  
▼ Monitor  
  ▶ System  
  ▶ Green Ethernet  
  ▶ Ports  
  ▶ DHCP  
  ▶ Security  
  ▼ LACP

LACP System Status

Auto-refresh ☐ Refresh

Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
No ports enabled or no existing partners					

Object	Description
<b>Aggr ID</b>	The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'
<b>Partner System ID</b>	The system ID (MAC address) of the aggregation partner.
<b>Partner Key</b>	The Key that the partner has assigned to this aggregation ID.
<b>Last Changed</b>	The time since this aggregation changed.
<b>Local Ports</b>	Shows which ports are a part of this aggregation for this switch.

Buttons	
	Click to refresh the page immediately.
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

## Port Status

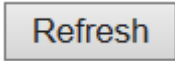
This page provides a status overview for [LACP](#) status for all ports.

**DIGISOL** DG-IS4508HP

- Configuration
- ▼ Monitor
  - System
  - Green Ethernet
  - Ports
  - ▼ DHCP
    - ▼ Server
      - Statistics
      - Binding
      - Declined IP
      - Snooping Table
      - Relay Statistics
      - Detailed Statistics
    - ▼ Security
      - Access Management
      - Statistics

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-

Object	Description
<b>Port</b>	The switch port number.
<b>LACP</b>	'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.
<b>Key</b>	The key assigned to this port. Only ports with the same key can aggregate together.
<b>Aggr ID</b>	The Aggregation ID assigned to this aggregation group.
<b>Partner System ID</b>	The partner's System ID (MAC address).
<b>Partner Port</b>	The partner's port number connected to this port.
<b>Partner Prio</b>	The partner's port priority.

Buttons	
	Click to refresh the page immediately.
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

## Port Statistics

This page provides an overview for [LACP](#) statistics for all ports.

The screenshot shows the DIGISOL DG-IS4508HP web interface. On the left is a navigation menu with the following items: Configuration, Monitor (expanded), System, Green Ethernet, Ports, DHCP (expanded), Server (expanded), Statistics, Binding, Declined IP, Snooping Table, Relay Statistics, Detailed Statistics, Security (expanded), Access Management, and Statistics. The main content area is titled 'LACP Statistics' and contains a table with the following data:

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0

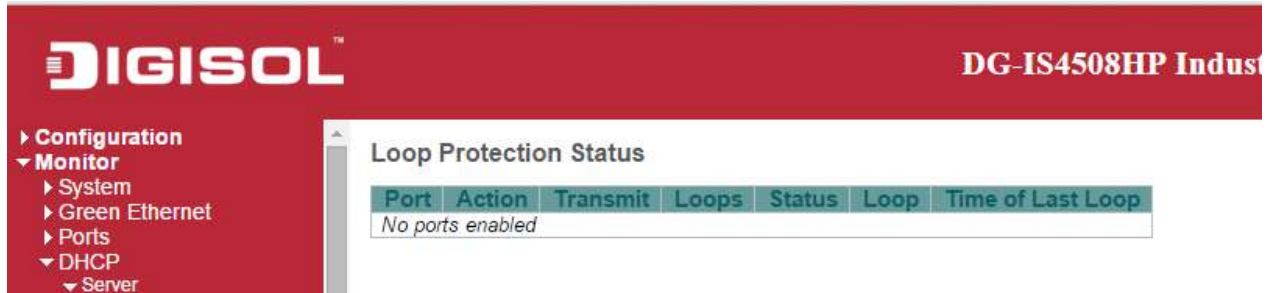
Object	Description
<b>Port</b>	The switch port number.
<b>LACP Received</b>	Shows how many LACP frames have been received at each port.
<b>LACP Transmitted</b>	Shows how many LACP frames have been sent from each port.
<b>Discarded</b>	Shows how many unknown or illegal LACP frames have been discarded at each port.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.
<input type="button" value="Clear"/>	Clears the counters for all ports.

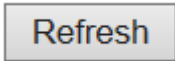


## Loop Protection

This page displays the loop protection port status the ports of the switch.



Object	Description
<b>Port</b>	The switch port number of the logical port.
<b>Action</b>	The currently configured port action.
<b>Transmit</b>	The currently configured port transmit mode.
<b>Loops</b>	The number of loops detected on this port.
<b>Status</b>	The current loop protection status of the port.
<b>Loop</b>	Whether a loop is currently detected on the port.
<b>Time of Last Loop</b>	The time of the last loop event detected.

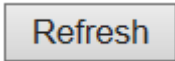
Buttons	
	Click to refresh the page immediately.
<b>Auto-refresh</b> <input type="checkbox"/>	Check this box to enable an automatic refresh of the page at regular intervals.

# Spanning Tree

## Bridge Status

This page provides a status overview of all [STP](#) bridge instances.

Object	Description
<b>MSTI</b>	The Bridge Instance. This is also a link to the <a href="#">STP Detailed Bridge Status</a> .
<b>Bridge ID</b>	The Bridge ID of this Bridge instance.
<b>Root ID</b>	The Bridge ID of the currently elected root bridge.
<b>Root Port</b>	The switch port currently assigned the <i>root</i> port role.
<b>Root Cost</b>	Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
<b>Topology Flag</b>	The current state of the Topology Change Flag of this Bridge instance.
<b>Topology Change Last</b>	The time since last Topology Change occurred.

Buttons	
	Click to refresh the page immediately.
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

## Port Status

This page displays the [STP](#) CIST port status for physical ports of the switch.

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	DesignatedPort	Forwarding	0d 01:10:23
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-

Object	Description
<b>Port</b>	The switch port number of the logical STP port.
<b>CIST Role</b>	The current STP port role of the CIST port. The port role can be one of the following values: <b>AlternatePort</b> <b>BackupPort</b> <b>RootPort</b> <b>DesignatedPort</b> <b>Disabled</b> .
<b>CIST State</b>	The current STP port state of the CIST port. The port state can be one of the following values: <b>Discarding</b> <b>Learning</b> <b>Forwarding</b> .
<b>Uptime</b>	The time since the bridge port was last initialized.

Buttons	
	Click to refresh the page immediately.
<b>Auto-refresh</b> <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

## Port Statistics

This page displays the [STP](#) port statistics counters of bridge ports in the switch.

**DIGISOL** DG-IS4508HP Industrial Ethernet Switch

Configuration  
Monitor  
System  
Green Ethernet  
Ports  
DHCP

STP Statistics

Auto-refresh ☐ Refresh Clear

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
5	2133	0	0	0	0	0	0	0	0	0

Object	Description
<b>Port</b>	The switch port number of the logical STP port.
<b>MSTP</b>	The number of MSTP BPDU's received/transmitted on the port.
<b>RSTP</b>	The number of RSTP BPDU's received/transmitted on the port.
<b>STP</b>	The number of legacy STP Configuration BPDU's received/transmitted on the port.
<b>TCN</b>	The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.
<b>Discarded Unknown</b>	The number of unknown Spanning Tree BPDU's received (and discarded) on the port.
<b>Discarded Illegal</b>	The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Buttons	
	Click to refresh the page immediately.
	Click to reset the counters.
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.



## MVR

### MVR Statistics

This page provides [MVR](#) Statistics information.

**DIGISOL™** DG-IS4508HP Industrial Ethernet Switch

Configuration  
Monitor  
System  
Green Ethernet  
Ports  
DHCP  
Security  
LACP

MVR Statistics

Auto-refresh ☐ Refresh Clear

VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
No more entries						

Object	Description
<b>VLAN ID</b>	The Multicast <a href="#">VLAN</a> ID.
<b>IGMP/MLD Queries Received</b>	The number of Received Queries for IGMP and MLD, respectively.
<b>IGMP/MLD Queries Transmitted</b>	The number of Transmitted Queries for IGMP and MLD, respectively.
<b>IGMPv1 Joins Received</b>	The number of Received IGMPv1 Join's.
<b>IGMPv2/MLDv1 Report's Received</b>	The number of Received IGMPv2 Join's and MLDv1 Report's, respectively.
<b>IGMPv3/MLDv2 Report's Received</b>	The number of Received IGMPv1 Join's and MLDv2 Report's, respectively.
<b>IGMPv2/MLDv1 Leave's Received</b>	The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively.

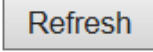
Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page immediately.
Clear	Clears all Statistics counters.





## MVR Channel Groups

Each page shows up to 99 entries from the MVR Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR Channels (Groups) Information Table.

The "Start from [VLAN](#)", and "Group Address" input fields allow the user to select the starting point in

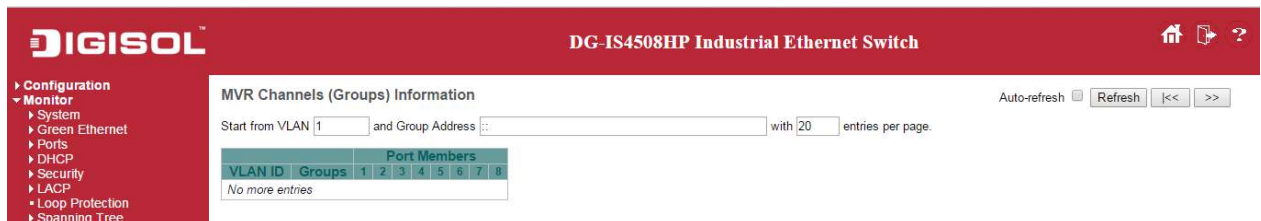
the MVR Channels (Groups) Information Table. Clicking the  button will update the displayed table starting from that or the closest next MVR Channels (Groups) Information Table match.

In addition, the two input fields will - upon a  button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

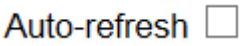
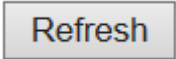
The  will use the last entry of the currently displayed table as a basis for the next lookup.

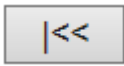

When the end is reached the text "No more entries" is shown in the displayed table. Use the

 button to start over.



Object	Description
<b>VLAN ID</b>	VLAN ID of the group.
<b>Groups</b>	Group ID of the group displayed.
<b>Port Members</b>	Ports under this group.

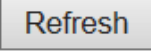
Buttons	
	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Refreshes the displayed table starting from the input fields.

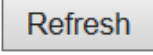
	<p>Updates the table starting from the first entry in the MVR Channels (Groups) Information Table.</p>
	<p>Updates the table, starting with the entry after the last entry currently displayed.</p>

## MVR SFM Information

Each page shows up to 99 entries from the MVR SFM Information Table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR SFM Information Table.

The "Start from [VLAN](#)", and "Group Address" input fields allow the user to select the starting point in

the MVR SFM Information Table. Clicking the  button will update the displayed table starting from that or the closest next MVR SFM Information Table match. In addition, the two input

fields will - upon a  button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The  will use the last entry of the currently displayed table as a basis for the next lookup.

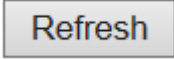
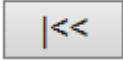

When the end is reached the text "No more entries" is shown in the displayed table. Use the

 button to start over.



Object	Description
<b>VLAN ID</b>	VLAN ID of the group.
<b>Group</b>	Group address of the group displayed.
<b>Port</b>	Switch port number.
<b>Mode</b>	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
<b>Source Address</b>	<a href="#">IP</a> Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is no any source filtering address, the text "None" is shown in the Source Address field.
<b>Type</b>	Indicates the Type. It can be either Allow or Deny.

<b>Hardware Filter/Switch</b>	Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.
-------------------------------	--

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Refreshes the displayed table starting from the input fields.
	Updates the table starting from the first entry in the MVR SFM Information Table.
	Updates the table, starting with the entry after the last entry currently displayed.

# IPMC

## IGMP Snooping

### IGMP Snooping Status

This page provides [IGMP](#) Snooping status.

**DIGISOL™** DG-IS4508HP Industrial Ethernet Switch

IGMP Snooping Status

Auto-refresh ☐ Refresh Clear

Statistics

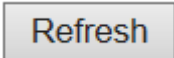
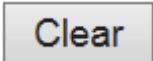
VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-

Object	Description
<b>VLAN ID</b>	The <a href="#">VLAN</a> ID of the entry.
<b>Querier Version</b>	Working Querier Version currently.
<b>Host Version</b>	Working Host Version currently.
<b>Querier Status</b>	Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.
<b>Querier Transmitted</b>	The number of Transmitted Queries.
<b>Queries Received</b>	The number of Received Queries.
<b>V1 Report Received</b>	The number of Received V1 Reports.
<b>V2 Report Received</b>	The number of Received V2 Reports.
<b>V3 Report Received</b>	The number of Received V3 Reports.
<b>V2 Leaves Received</b>	The number of Received V2 Leaves.
<b>Router Port</b>	Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or <a href="#">IGMP querier</a> . Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.

<b>Port</b>	Switch port number.
<b>Status</b>	Indicate whether specific port is a router port or not.

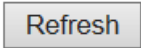
Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Click to refresh the page immediately.
	Clears all Statistics counters.

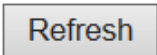


## Groups Information


Each page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table.

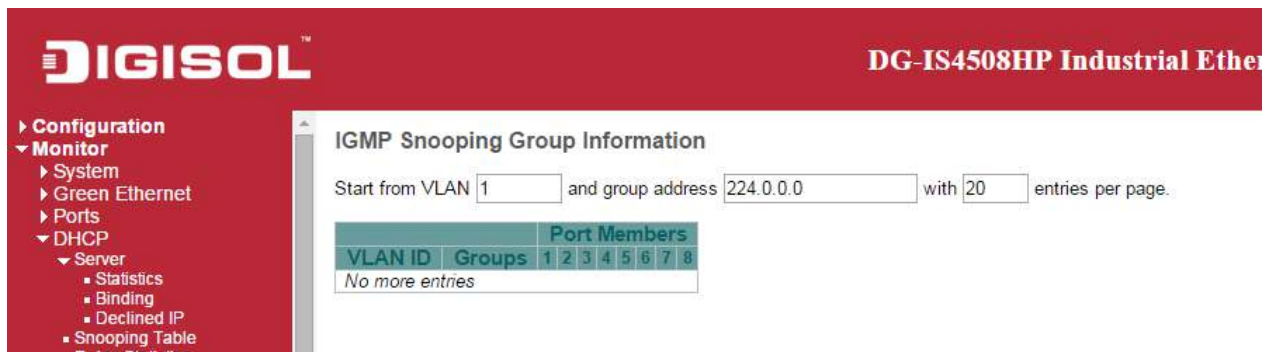
The "Start from [VLAN](#)", and "group" input fields allow the user to select the starting point in the IGMP

Group Table. Clicking the  button will update the displayed table starting from that or the

closest next IGMP Group Table match. In addition, the two input fields will - upon a  button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

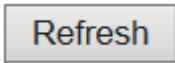
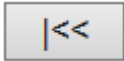

The  will use the last entry of the currently displayed table as a basis for the next lookup.

When the end is reached the text "No more entries" is shown in the displayed table. Use the  button to start over.



Object	Description
<b>VLAN ID</b>	VLAN ID of the group.
<b>Groups</b>	Group address of the group displayed.
<b>Port Members</b>	Ports under this group.

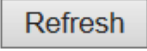
Buttons	
<b>Auto-refresh</b> <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

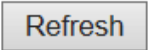
	<p>Refreshes the displayed table starting from the input fields.</p>
	<p>Updates the table, starting with the first entry in the IGMP Group Table.</p>
	<p>Updates the table, starting with the entry after the last entry currently displayed.</p>

## IPv4 SFM Information


Each page shows up to 99 entries from the IGMP SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP SFM Information Table.

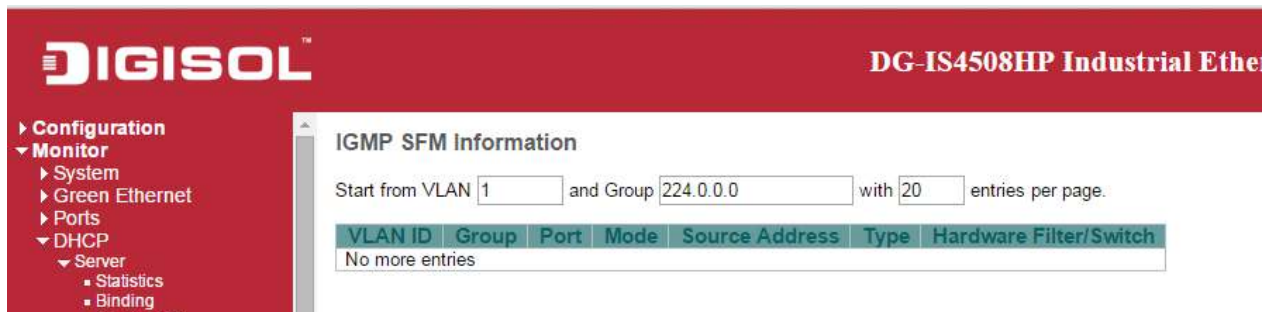
The "Start from [VLAN](#)", and "group" input fields allow the user to select the starting point in the IGMP

SFM Information Table. Clicking the  button will update the displayed table starting from that or the closest next IGMP SFM Information Table match. In addition, the two input fields will - upon

a  button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

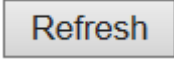
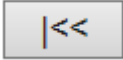

The  will use the last entry of the currently displayed table as a basis for the next lookup.

When the end is reached the text "No more entries" is shown in the displayed table. Use the  button to start over.



Object	Description
<b>VLAN ID</b>	VLAN ID of the group.
<b>Group</b>	Group address of the group displayed.
<b>Port</b>	Switch port number.
<b>Mode</b>	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
<b>Source Address</b>	<a href="#">IP</a> Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
<b>Type</b>	Indicates the Type. It can be either Allow or Deny.

<b>Hardware Filter/Switch</b>	Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.
-------------------------------	---

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Refreshes the displayed table starting from the input fields.
	Updates the table starting from the first entry in the IGMP SFM Information Table.
	Updates the table, starting with the entry after the last entry currently displayed.

## MLD Snooping

### MLD Snooping Status

This page provides [MLD](#) Snooping status.

**DIGISOL™** DG-IS4508HP Industrial Ethernet Switch

Configuration  
 Monitor  
 System  
 Green Ethernet  
 Ports  
 DHCP  
 Server  
 Statistics  
 Binding  
 Declined IP  
 Snooping Table  
 Relay Statistics  
 Detailed Statistics  
 Security  
 Access Management  
 Statistics  
 Network  
 Port Security  
 Switch  
 Port  
 NAS  
 ACL Status

#### MLD Snooping Status

Statistics



VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received
1	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-

Object	Description
<b>VLAN ID</b>	The <a href="#">VLAN</a> ID of the entry.
<b>Querier Version</b>	Working Querier Version currently.
<b>Host Version</b>	Working Host Version currently.
<b>Querier Status</b>	Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.
<b>Queries Transmitted</b>	The number of Transmitted Queries.
<b>Queries Received</b>	The number of Received Queries.
<b>V1 Report Received</b>	The number of Received V1 Reports.
<b>V2 Report Received</b>	The number of Received V2 Reports.
<b>V1 Leaves Received</b>	The number of Received V1 Leaves.
<b>Router Port</b>	Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or <a href="#">MLD querier</a> . Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.
<b>Port</b>	Switch port number.

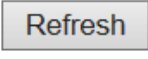
<b>status</b>	Indicate whether specific port is a router port or not.
---------------	---

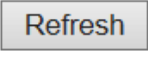
Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Click to refresh the page immediately.
	Clears all Statistics counters.

## Groups Information


Each page shows up to 99 entries from the MLD Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table.

The "Start from [VLAN](#)", and "group" input fields allow the user to select the starting point in the MLD

Group Table. Clicking the  button will update the displayed table starting from that or the

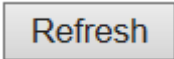
closest next MLD Group Table match. In addition, the two input fields will - upon a  button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

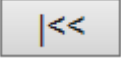
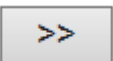
The  will use the last entry of the currently displayed table as a basis for the next lookup.

When the end is reached the text "No more entries" is shown in the displayed table. Use the  button to start over.



Object	Description
<b>VLAN ID</b>	VLAN ID of the group.
<b>Groups</b>	Group address of the group displayed.
<b>Port Members</b>	Ports under this group.

Buttons	
<b>Auto-refresh</b> <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Refreshes the displayed table starting from the input fields.

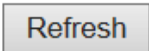
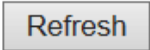
	<p>Updates the table, starting with the first entry in the MLD Group Table.</p>
	<p>Updates the table, starting with the entry after the last entry currently displayed.</p>




## IPv6 SFM Information

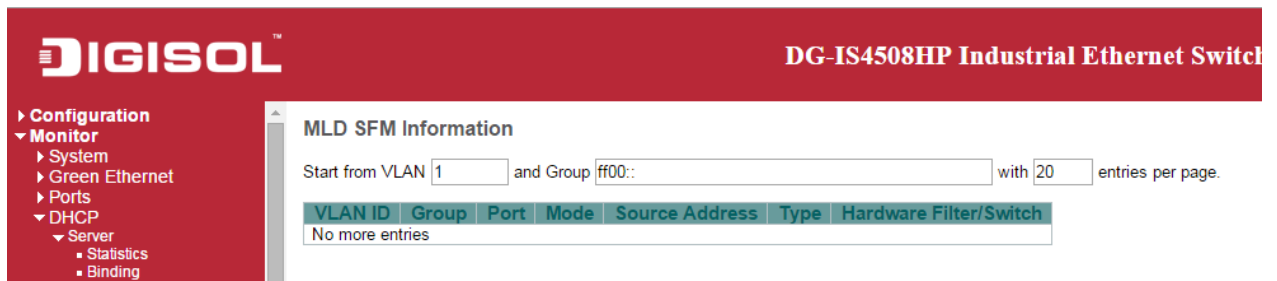
Each page shows up to 99 entries from the MLD SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD SFM Information Table.

The "Start from [VLAN](#)", and "group" input fields allow the user to select the starting point in the MLD

SFM Information Table. Clicking the  button will update the displayed table starting from that or the closest next MLD SFM Information Table match. In addition, the two input fields will - upon a  button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.


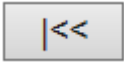

The  will use the last entry of the currently displayed table as a basis for the next lookup.

When the end is reached the text "No more entries" is shown in the displayed table. Use the  button to start over.



Object	Description
<b>VLAN ID</b>	VLAN ID of the group.
<b>Group</b>	Group address of the group displayed.
<b>Port</b>	Switch port number.
<b>Mode</b>	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
<b>Source Address</b>	<a href="#">IP</a> Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
<b>Type</b>	Indicates the Type. It can be either Allow or Deny.
<b>Hardware Filter/Switch</b>	Indicates whether data plane destined to the specific group address from the source

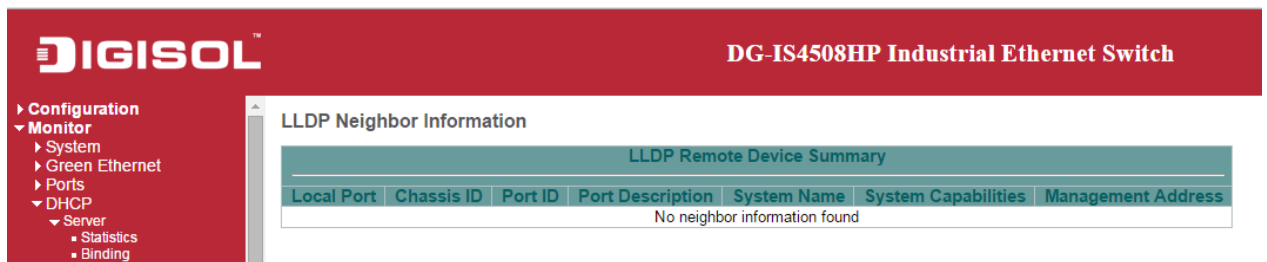
	IPv6 address could be handled by chip or not.
--	---

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Refreshes the displayed table starting from the input fields..
	Updates the table starting from the first entry in the MLD SFM Information Table.
	Updates the table, starting with the entry after the last entry currently displayed.

## LLDP

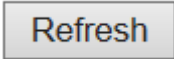
### Neighbors

This page provides a status overview for all [LLDP](#) neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected.



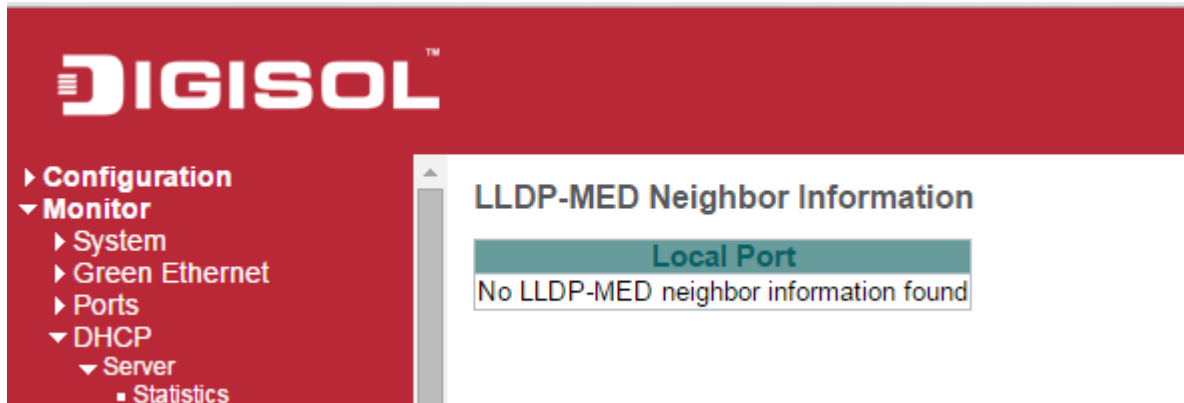
Object	Description
<b>Local Port</b>	The port on which the LLDP frame was received.
<b>Chassis ID</b>	The <b>Chassis ID</b> is the identification of the neighbor's LLDP frames.
<b>Port ID</b>	The <b>Port ID</b> is the identification of the neighbor port.
<b>Port Description</b>	<b>Port Description</b> is the port description advertised by the neighbor unit.
<b>System Name</b>	<b>System Name</b> is the name advertised by the neighbor unit.
<b>System Capabilities</b>	<p><b>System Capabilities</b> describes the neighbor unit's capabilities. The possible capabilities are:</p> <ol style="list-style-type: none"> <li>1. Other</li> <li>2. Repeater</li> <li>3. Bridge</li> <li>4. WLAN Access Point</li> <li>5. Router</li> <li>6. Telephone</li> <li>7. DOCSIS cable device</li> </ol>

	<p>8. Station only</p> <p>9. Reserved</p> <p>When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).</p>
<b>Management Address</b>	<p><b>Management Address</b> is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address.</p>

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Click to refresh the page.

## LLDP-MED Neighbors

This page provides a status overview of all [LLDP-MED](#) neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. This function applies to VoIP devices which support LLDP-MED.



Object	Description
<b>Port</b>	The port on which the LLDP frame was received.
<b>Device Type</b>	<p>LLDP-MED Devices are comprised of two primary <b>Device Types</b>: Network Connectivity Devices and Endpoint Devices.</p> <p><b>LLDP-MED Network Connectivity Device Definition</b></p> <p>LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:</p> <ol style="list-style-type: none"> <li>1. LAN Switch/Router</li> <li>2. IEEE 802.1 Bridge</li> <li>3. IEEE 802.3 Repeater (included for historical reasons)</li> <li>4. IEEE 802.11 Wireless Access Point</li> </ol>

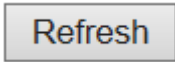
	<p>5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.</p> <p><b>LLDP-MED Endpoint Device Definition</b></p> <p>LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.</p> <p>Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.</p> <p>Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).</p> <p><b>LLDP-MED Generic Endpoint (Class I)</b></p> <p>The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.</p> <p>Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.</p> <p><b>LLDP-MED Media Endpoint (Class II)</b></p> <p>The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects</p>
--	---

	<p>related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.</p> <p>Discovery services defined in this class include media-type-specific network layer policy discovery.</p> <p><b>LLDP-MED Communication Endpoint (Class III)</b></p> <p>The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.</p> <p>Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.</p>
<b>LLDP-MED Capabilities</b>	<p><b>LLDP-MED Capabilities</b> describes the neighbor unit's LLDP-MED capabilities. The possible capabilities are:</p> <ol style="list-style-type: none"> <li>1. LLDP-MED capabilities</li> <li>2. Network Policy</li> <li>3. Location Identification</li> <li>4. Extended Power via MDI - PSE</li> <li>5. Extended Power via MDI - PD</li> <li>6. Inventory</li> <li>7. Reserved</li> </ol>
<b>Application Type</b>	<b>Application Type</b> indicating the primary function of the application(s) defined for this

	<p>network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.</p> <ol style="list-style-type: none"> <li>1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.</li> <li>2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media.</li> <li>3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.</li> <li>4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.</li> <li>5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.</li> <li>6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.</li> <li>7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.</li> <li>8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media.</li> </ol>
<b>Policy</b>	<p><b>Policy</b> indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown</p> <p>Unknown: The network policy for the specified application type is currently unknown.</p> <p>Defined: The network policy is defined.</p>
<b>TAG</b>	<p><b>TAG</b> is indicative of whether the specified application type is using a tagged or an</p>




	<p>untagged VLAN. Can be Tagged or Untagged.</p> <p>Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.</p> <p>Tagged: The device is using the IEEE 802.1Q tagged frame format.</p>
<b>VLAN ID</b>	<b>VLAN ID</b> is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.
<b>Priority</b>	<b>Priority</b> is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).
<b>DSCP</b>	<b>DSCP</b> is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).
<b>Auto-negotiation</b>	<b>Auto-negotiation</b> identifies if MAC/PHY auto-negotiation is supported by the link partner.
<b>Auto-negotiation status</b>	<b>Auto-negotiation status</b> identifies if auto-negotiation is currently enabled at the link partner. If <b>Auto-negotiation</b> is supported and <b>Auto-negotiation status</b> is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.
<b>Auto-negotiation Capabilities</b>	<b>Auto-negotiation Capabilities</b> shows the link partners MAC/PHY capabilities.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Click to refresh the page.

## EEE

By using [EEE](#) power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits [EEE](#) turn off to save power, need time to boot up before sending traffic over the link. This time is called "wake up time". To achieve minimal latency, devices can use [LLDP](#) to exchange information about their respective tx and rx "wake up time ", as a way to agree upon the minimum wakeup time they need.

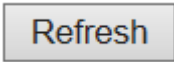
This page provides an overview of [EEE](#) information exchanged by [LLDP](#).



Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
No LLDP EEE information found								

Object	Description
<b>Local Port</b>	The port on which <a href="#">LLDP</a> frames are received or transmitted.
<b>Tx Tw</b>	The link partner's maximum time that transmit path can hold-off sending data after deassertion of LPI.
<b>Rx Tw</b>	The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.
<b>Fallback Receive Tw</b>	<p>The link partner's fallback receive Tw.</p> <p>A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.</p>
<b>Echo Tx Tw</b>	<p>The link partner's Echo Tx Tw value.</p> <p>The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values.</p>

	For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.
<b>Echo Rx Tw</b>	The link partner's Echo Rx Tw value.
<b>Resolved Tx Tw</b>	The resolved Tx Tw for this link. Note : NOT the link partner  The resolved value that is the actual "tx wakeup time " used for this link (based on <a href="#">EEE</a> information exchanged via <a href="#">LLDP</a> ).
<b>Resolved Rx Tw</b>	The resolved Rx Tw for this link. Note : NOT the link partner  The resolved value that is the actual "tx wakeup time " used for this link (based on <a href="#">EEE</a> information exchanged via <a href="#">LLDP</a> ).
<b>EEE in Sync</b>	Shows whether the switch and the link partner have agreed on wake times.  Red - Switch and link partner have not agreed on wakeup times.  Green - Switch and link partner have agreed on wakeup times.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Click to refresh the page.

## Port Statistics

This page provides an overview of all [LLDP](#) traffic.

Two types of counters are shown. **Global counters** are counters that refer to the whole switch, while **local counters** refer to per port counters for the currently selected switch.

The screenshot shows the web interface of a DIGISOL DG-IS4508HP Industrial Ethernet Switch. The left sidebar contains a navigation menu with categories like Configuration, Monitor, System, Green Ethernet, Ports, DHCP, Security, LACP, Loop Protection, Spanning Tree, MVR, IPMC, LLDP, PoE, MAC Table, VLANs, VCL, sFlow, RingV2, DDMI, Diagnostics, and Maintenance. The main content area displays LLDP statistics. At the top, there's a section for 'LLDP Global Counters' with a table showing global statistics. Below that, there's a section for 'LLDP Statistics Local Counters' with a table showing per-port statistics for ports 1 through 8. The interface includes a red header bar with the DIGISOL logo and the device name, and a right sidebar with icons for home, refresh, and help.

**LLDP Global Counters**

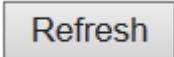
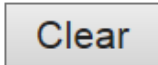
Global Counters	
Neighbor entries were last changed	1999-12-31T23:59:58+00:00 (7944 secs. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

**LLDP Statistics Local Counters**

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	265	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

Object	Description
<b>Global Counters</b>	
<b>Neighbor entries were last change</b>	Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.
<b>Total Neighbors Entries Added</b>	Shows the number of new entries added since switch reboot.
<b>Total Neighbors Entries Deleted</b>	Shows the number of new entries deleted since switch reboot.
<b>Total Neighbors Entries Dropped</b>	Shows the number of <a href="#">LLDP</a> frames dropped due to the entry table being full.
<b>Total Neighbors Entries Aged Out</b>	Shows the number of entries deleted due to Time-To-Live expiring.
<b>Local Counters</b>	
<b>Local Port</b>	The port on which <a href="#">LLDP</a> frames are received or transmitted.
<b>Tx Frames</b>	The number of <a href="#">LLDP</a> frames transmitted on the port.

<b>Rx Frames</b>	The number of <a href="#">LLDP</a> frames received on the port.
<b>Rx Errors</b>	The number of received <a href="#">LLDP</a> frames containing some kind of error.
<b>Frames Discarded</b>	If a <a href="#">LLDP</a> frame is received on a port, and the switch's internal table has run full, the <a href="#">LLDP</a> frame is counted and discarded. This situation is known as "Too Many Neighbors" in the <a href="#">LLDP</a> standard. <a href="#">LLDP</a> frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an <a href="#">LLDP</a> shutdown frame is received, or when the entry ages out.
<b>TLVs Discarded</b>	Each <a href="#">LLDP</a> frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
<b>TLVs Unrecognized</b>	The number of well-formed TLVs, but with an unknown type value.
<b>Org. Discarded</b>	If <a href="#">LLDP</a> frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted.
<b>Age-Outs</b>	Each <a href="#">LLDP</a> frame contains information about how long time the <a href="#">LLDP</a> information is valid (age-out time). If no new <a href="#">LLDP</a> frame is received within the age out time, the <a href="#">LLDP</a> information is removed, and the <b>Age-Out</b> counter is incremented.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Click to refresh the page.
	Clears the <b>local counters</b> . All counters (including <b>global counters</b> ) are cleared upon reboot.

## PoE

This page allows the user to inspect the current status for all [PoE](#) ports.

DIGISOL™		DG-IS4508HP Industrial Ethernet Switch					
<ul style="list-style-type: none"> <li>Configuration</li> <li>Monitor               <ul style="list-style-type: none"> <li>System</li> <li>Green Ethernet</li> <li>Ports</li> <li>DHCP                   <ul style="list-style-type: none"> <li>Server                       <ul style="list-style-type: none"> <li>Statistics</li> <li>Binding</li> <li>Declined IP</li> <li>Snooping Table</li> <li>Relay Statistics</li> </ul> </li> </ul> </li> </ul> </li> </ul>		Power Over Ethernet Status					
Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
3	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

Object	Description
<b>PoE Status</b>	
<b>Local Port</b>	This is the logical port number for this row.
<b>PD Class</b>	<p>Each PD is classified according to a class that defines the maximum power the PD will use. The PD Class shows the PDs class.</p> <p>Five Classes are defined:</p> <p>Class 0: Max. power 15.4 W</p> <p>Class 1: Max. power 4.0 W</p> <p>Class 2: Max. power 7.0 W</p> <p>Class 3: Max. power 15.4 W</p> <p>Class 4: Max. power 30.0 W</p>
<b>Power Requested</b>	The Power Requested shows the requested amount of power the PD wants to be reserved.
<b>Power Allocated</b>	The Power Allocated shows the amount of power the switch has allocated for the PD.
<b>Power Used</b>	The Power Used shows how much power the PD currently is using.
<b>Current Used</b>	The Power Used shows how much current the PD currently is using.
<b>Priority</b>	The Priority shows the port's priority configured by the user.
<b>Port Status</b>	<p>The Port Status shows the port's status. The status can be one of the following values:</p> <p><b>PoE not available - No PoE chip found</b> - PoE not supported for the port.</p> <p><b>PoE turned OFF - PoE disabled</b> - PoE is disabled by user.</p> <p><b>PoE turned OFF - Power budget exceeded</b> - The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down.</p> <p><b>No PD detected</b> - No PD detected for the port.</p>

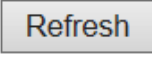
	<p><b>PoE turned OFF - PD overload</b> - The PD has requested or used more power than the port can deliver, and is powered down.</p> <p><b>PoE turned OFF</b> - PD is off.</p> <p><b>Invalid PD</b> - PD detected, but is not working correctly.</p>
--	--


Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page.


## MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

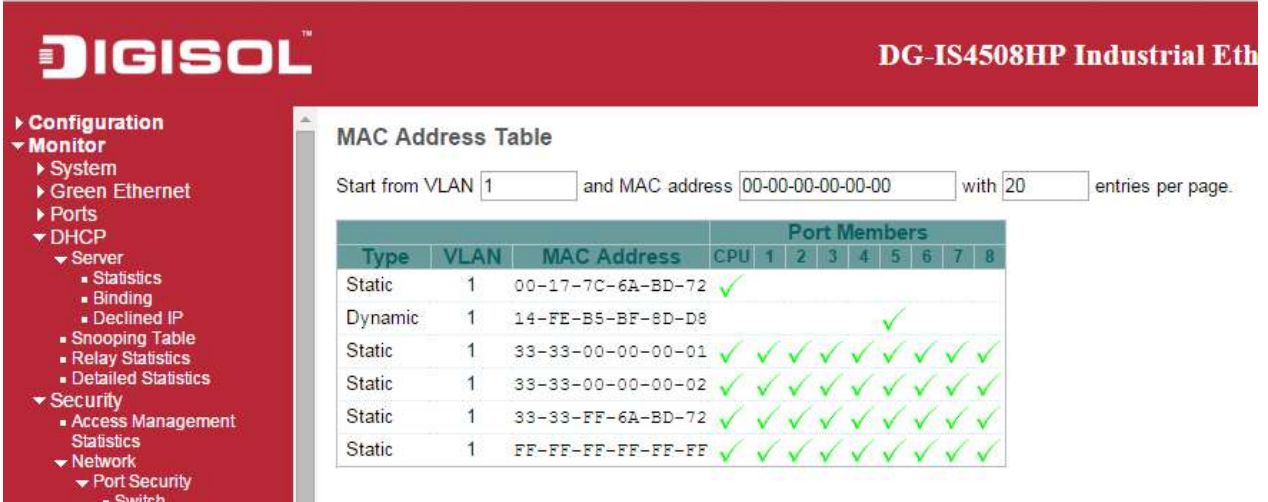
The "Start from MAC address" and "VLAN" input fields allow the user to select the starting point in the

MAC Table. Clicking the  button will update the displayed table starting from that or the

closest next MAC Table match. In addition, the two input fields will - upon a  button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The  will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table.

Use the  button to start over.



**DIGISOL** DG-IS4508HP Industrial Eth

► Configuration  
▼ Monitor  
  ► System  
  ► Green Ethernet  
  ► Ports  
  ▼ DHCP  
    ▼ Server  
      ▪ Statistics  
      ▪ Binding  
      ▪ Declined IP  
      ▪ Snooping Table  
      ▪ Relay Statistics  
      ▪ Detailed Statistics  
  ▼ Security  
    ▪ Access Management  
    Statistics  
  ▼ Network  
    ▼ Port Security  
      ▪ Switch

**MAC Address Table**


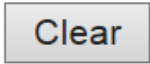
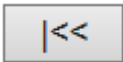

Start from VLAN  and MAC address  with  entries per page.

Type	VLAN	MAC Address	Port Members								
			CPU	1	2	3	4	5	6	7	8
Static	1	00-17-7C-6A-BD-72	✓								
Dynamic	1	14-FE-B5-BF-8D-D8						✓			
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-6A-BD-72	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓

Object	Description
<b>Switch (stack only)</b>	The stack unit where the entry is learned.
<b>Type</b>	Indicates whether the entry is a static or a dynamic entry.
<b>MAC Address</b>	The MAC address of the entry.



<b>VLAN</b>	The VLAN ID of the entry.
<b>Port Members</b>	The ports that are members of the entry.

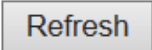
Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.
	Flushes all dynamic entries.
	Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.
	Updates the table, starting with the entry after the last entry currently displayed.


## VLANs

### VLANs Membership

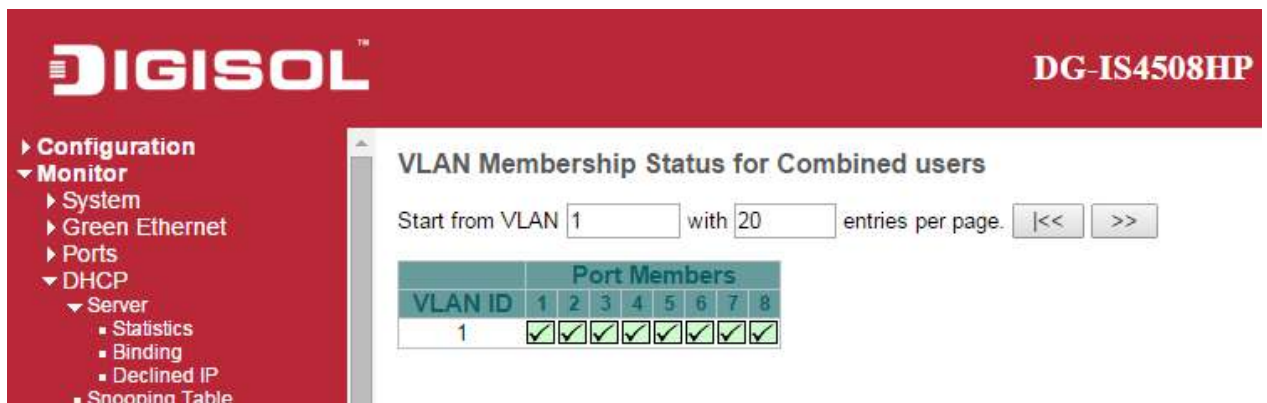
Each page shows up to 99 entries from the VLAN table (default being 20), selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input field allows the user to select the starting point in the VLAN Table.




Clicking the  button will update the displayed table starting from that or the closest next VLAN Table match.

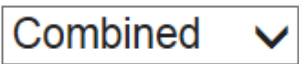
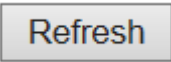
The  will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached, the text "No data exists for the selected user" is shown in the table.

Use the  button to start over.



Object	Description
<b>VLAN User</b>	<p>Various internal software modules may use VLAN services to configure VLAN memberships on the fly.</p> <p>The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.</p> <p>The "Combined" entry will show a combination of the administrator and internal</p>

	software modules configuration, and basically reflects what is actually configured in hardware.
<b>VLAN ID</b>	VLAN ID for which the Port members are displayed.
<b>Port Members</b>	<p>A row of check boxes for each port is displayed for each VLAN ID.</p> <p>If a port is included in a VLAN, the following image will be displayed: .</p> <p>If a port is in the forbidden port list, the following image will be displayed: .</p> <p>If a port is in the forbidden port list and at the same time attempted included in the VLAN, the following image will be displayed: . The port will not be a member of the VLAN in this case.</p>

Buttons	
	Select VLAN Users from this drop down list.
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Click to refresh the page immediately.

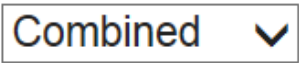
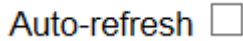
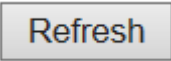
## VLANs Ports

This page provides [VLAN](#) Port Status.

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
2	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
3	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
4	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
5	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
6	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
7	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
8	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No

Object	Description
<b>VLAN User</b>	<p>Various internal software modules may use VLAN services to configure VLAN port configuration on the fly.</p> <p>The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.</p> <p>The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.</p> <p>If a given software modules hasn't overridden any of the port settings, the text "No data exists for the selected user" is shown in the table.</p>
<b>Port</b>	The logical port for the settings contained in the same row.
<b>Port Type</b>	<p>Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port.) that a given user wants to configure on the port.</p> <p>The field is empty if not overridden by the selected user.</p>
<b>Ingress Filtering</b>	<p>Shows whether a given user wants ingress filtering enabled or not.</p> <p>The field is empty if not overridden by the selected user.</p>
<b>Frame Type</b>	<p>Shows the acceptable frame types (All, Taged, Untagged) that a given user wants to configure on the port.</p> <p>The field is empty if not overridden by the selected user.</p>
<b>Port VALN ID</b>	Shows the Port VLAN ID (PVID) that a given user wants the port to have.

	The field is empty if not overridden by the selected user.
<b>Tx Tag</b>	Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port.  The field is empty if not overridden by the selected user.
<b>Untagged VLAN ID</b>	If Tx Tag is overridden by the selected user and is set to Tag or Untag UVID, then this field will show the VLAN ID the user wants to tag or untag on egress.  The field is empty if not overridden by the selected user.
<b>Conflicts</b>	Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress.  Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list: The higher in the list, the higher priority.  If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module.  The "Combined" user reflects what is actually configured in hardware.

Buttons	
	Select VLAN Users from this drop down list.
	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Click to refresh the page immediately.

## VCL

### MAC-Based VLAN

This page shows MAC-based VLAN entries configured by various MAC-based VLAN users. Currently we support following VLAN User types:

CLI/Web/SNMP : These are referred to as static.

NAS : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

Object	Description
<b>MAC Address</b>	Indicates the MAC address.
<b>VLAN ID</b>	Indicates the VLAN ID.
<b>Port Members</b>	Port members of the MAC-based VLAN entry.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
<input type="button" value="Refresh"/>	Refreshes the displayed table.

## sFlow

This page shows receiver and per-port [sFlow](#) statistics.

**DIGISOL™** **DG-IS4508HP**

**Configuration**  
**Monitor**  
 ▶ System  
 ▶ Green Ethernet  
 ▶ Ports  
 ▼ DHCP  
   ▶ Server  
     ▪ Statistics  
     ▪ Binding  
     ▪ Declined IP  
     ▪ Snooping Table  
     ▪ Relay Statistics  
     ▪ Detailed Statistics  
 ▶ Security  
 ▶ LACP  
 ▶ Loop Protection  
 ▶ Spanning Tree  
 ▶ MVR  
 ▶ IPMC  
 ▶ LLDP  
 ▶ PoE  
 ▶ MAC Table  
 ▼ VLANs  
   ▪ Membership  
   ▪ Ports  
 ▼ VCL  
   ▪ MAC-based VLAN

**sFlow Statistics**

**Receiver Statistics**

Owner	<none>
IP Address/Hostname	0.0.0.0
Timeout	0
Tx Successes	0
Tx Errors	0
Flow Samples	0
Counter Samples	0

**Port Statistics**

Port	Rx Flow Samples	Tx Flow Samples	Counter Samples
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	0
8	0	0	0

Object	Description
<b>Receiver Statistics</b>	
<b>Owner</b>	<p>This field shows the current owner of the sFlow configuration. It assumes one of three values as follows:</p> <ul style="list-style-type: none"> <li>• If sFlow is currently unconfigured/unclaimed, Owner contains <b>&lt;none&gt;</b>.</li> <li>• If sFlow is currently configured through Web or CLI, Owner contains <b>&lt;Configured through local management&gt;</b>.</li> <li>• If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.</li> </ul>
<b>IP Address/Hostname</b>	The IP address or hostname of the sFlow receiver.
<b>Timeout</b>	The number of seconds remaining before sampling stops and the current sFlow owner is released.
<b>Tx Successes</b>	The number of UDP datagrams successfully sent to the sFlow receiver.

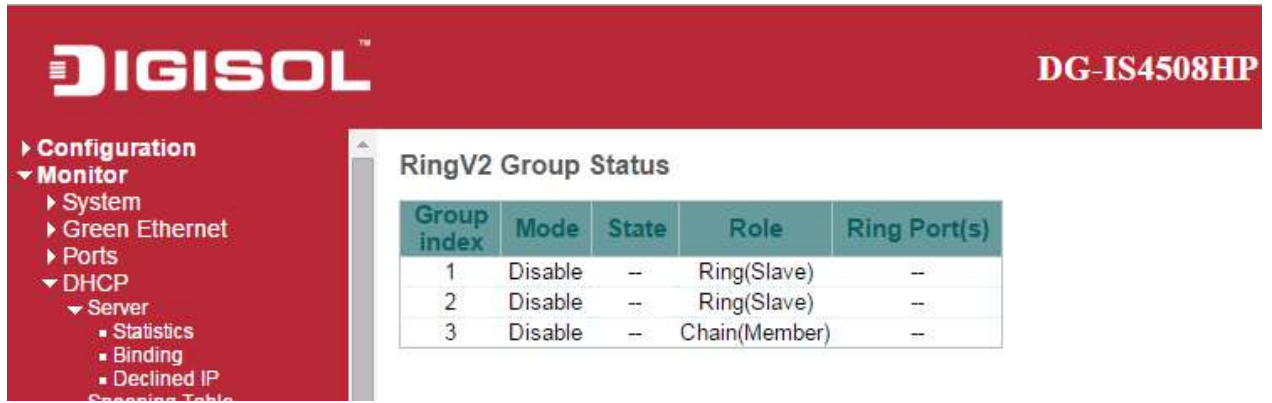
<b>Tx Errors</b>	The number of UDP datagrams that has failed transmission.  The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics → Ping/Ping6).
<b>Flow Samples</b>	The total number of flow samples sent to the sFlow receiver.
<b>Counter Samples</b>	The total number of counter samples sent to the sFlow receiver.
<b>Port Statistics</b>	
<b>Port</b>	The port number for which the following statistics applies.
<b>Rx and Tx Flow Samples</b>	The number of flow samples sent to the sFlow receiver originating from this port.  Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.
<b>Counter Samples</b>	The total number of counter samples sent to the sFlow receiver originating from this port.

<b>Buttons</b>	
<b>Auto-refresh</b> <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
<b>Refresh</b>	Click to refresh the page.
<b>Clear Receiver</b>	Clears the sFlow receiver counters.
<b>Clear Ports</b>	Clears the per-port counters.



## RingV2

This page provides a status overview for all of Ring status.



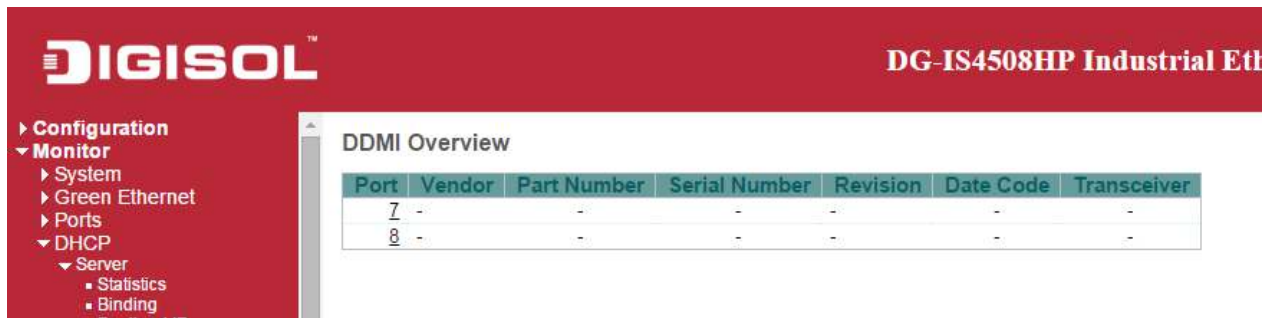
Group index	Mode	State	Role	Ring Port(s)
1	Disable	--	Ring(Slave)	--
2	Disable	--	Ring(Slave)	--
3	Disable	--	Chain(Member)	--

Object	Description
<b>Group Index</b>	The group index. This parameter is used for easy identifying which ring group.
<b>Mode</b>	It indicates whether the group is enabled.
<b>Role</b>	It indicates group is configured as which role.
<b>State</b>	When ring is complete, it will show " <b>Normal</b> ".  When ring is incomplete (at least one link is down), it will show " <b>Fail</b> ".
<b>Ring Port(s)</b>	Describes current status of ring port(s).

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page.

## DDMI Overview

Display [DDMI](#) overview information on this page.



Object	Description
<b>Port</b>	DDMI port.
<b>Vendor</b>	Indicates Vendor name SFP vendor name.
<b>Part Number</b>	Indicates Vendor PN Part number provided by SFP vendor.
<b>Serial Number</b>	Indicates Vendor SN Serial number provided by vendor.
<b>Revision</b>	Indicates Vendor rev Revision level for part number provided by vendor.
<b>Date Code</b>	Indicates Date code Vendor's manufacturing date code.
<b>Transceiver</b>	Indicates Transceiver compatibility.

## DDMI Detailed

Display [DDMI](#) detailed information on this page.

DG-IS4508HP Industrial Ethernet Switch

Configuration

Monitor

- System
- Green Ethernet
- Ports
- DHCP
- Security
- LACP
- Loop Protection
- Spanning Tree
- MVR
- IPMC
- LLDP
- Port
- MAC Table
- VLANs
- VCL
- sFlow
- RingV2
- DDMI
  - Overview
  - Detailed

Transceiver Information

Port 7 ▾ Auto-refresh ☐ Refresh

Vendor	-
Part Number	-
Serial Number	-
Revision	-
Date Code	-
Transceiver	-

DDMI Information

Type	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)	-	-	-	-	-
Voltage(V)	-	-	-	-	-
Tx Bias(mA)	-	-	-	-	-
Tx Power(dBm)	-	-	-	-	-
Rx Power(dBm)	-	-	-	-	-

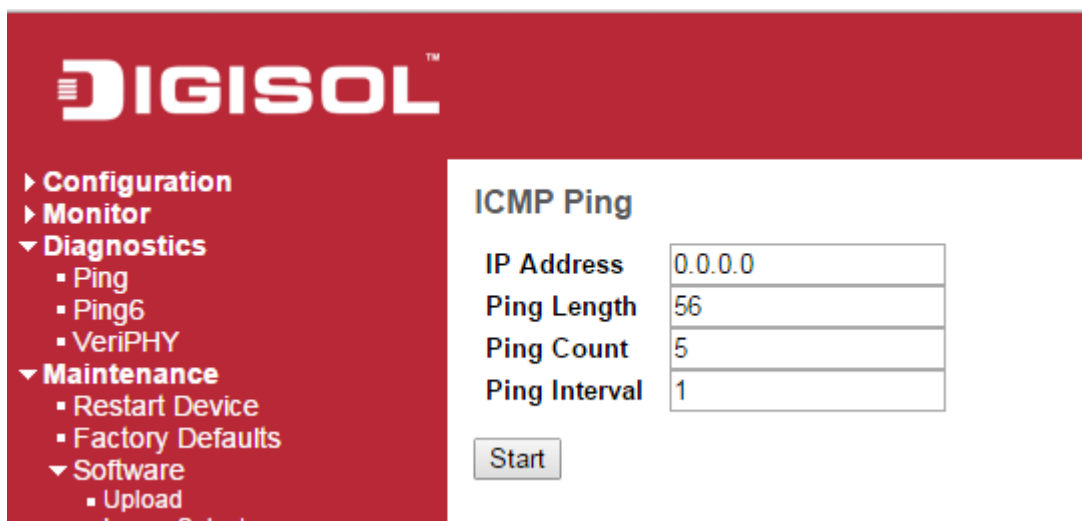
Object	Description
<b>Transceiver Information</b>	
<b>Vendor</b>	Indicates Vendor name SFP vendor name.
<b>Part Number</b>	Indicates Vendor PN Part number provided by SFP vendor.
<b>Serial Number</b>	Indicates Vendor SN Serial number provided by vendor.
<b>Revision</b>	Indicates Vendor rev Revision level for part number provided by vendor.
<b>Date Code</b>	Indicates Date code Vendor's manufacturing date code.
<b>Transceiver</b>	Indicates Transceiver compatibility.
<b>DDMI Information</b>	
<b>Current</b>	The current value of temperature, voltage, TX bias, TX power, and RX power.
<b>High Alarm Threshold</b>	The high alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.
<b>High Warn Threshold</b>	The high warn threshold value of temperature, voltage, TX bias, TX power, and RX power.
<b>Low Warn Threshold</b>	The low warn threshold value of temperature, voltage, TX bias, TX power, and RX power.
<b>Low Alarm Threshold</b>	The low alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page.

## Diagnostics

### Ping

This page allows you to issue [ICMP PING](#) packets to troubleshoot [IP](#) connectivity issues.





The screenshot shows the DIGISOL web interface. On the left is a navigation menu with the following items: Configuration, Monitor, Diagnostics (expanded), and Maintenance. Under Diagnostics, there are sub-items: Ping, Ping6, and VeriPHY. Under Maintenance, there are sub-items: Restart Device, Factory Defaults, Software, and Upload. The main content area is titled 'ICMP Ping' and contains four input fields: IP Address (0.0.0.0), Ping Length (56), Ping Count (5), and Ping Interval (1). Below these fields is a 'Start' button.

### ICMP Ping Output

PING server 0.0.0.0, 56 bytes of data.  
recvfrom: Operation timed out  
recvfrom: Operation timed out  
recvfrom: Operation timed out  
recvfrom: Operation timed out  
recvfrom: Operation timed out  
Sent 5 packets, received 0 OK, 0 bad

New Ping

Object	Description
<b>IP Address</b>	The destination IP Address.
<b>Ping Length</b>	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
<b>Ping Count</b>	The count of the ICMP packet. Values range from 1 time to 60 times.
<b>Ping Interval</b>	The interval of the ICMP packet. Values range from 0 second to 30 seconds.
<b>Egress Interface (only for IPv6)</b>	<p>The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.</p> <p>When the egress interface is not given, PING6 finds the best match interface for destination.</p> <p>Do not specify egress interface for loopback address.</p> <p>Do specify egress interface for link-local or multicast address.</p>

Buttons	
	Click to start transmitting ICMP packets.
	Click to re-start diagnostics with PING.

## Ping6

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

## ICMPv6 Ping Output

PING6 server ::, 56 bytes of data.

sendto

sendto

sendto

sendto



sendto

Sent 0 packets, received 0 OK, 0 bad

New Ping

Object	Description
<b>IP Address</b>	The destination IP Address.
<b>Ping Length</b>	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
<b>Ping Count</b>	The count of the ICMP packet. Values range from 1 time to 60 times.
<b>Ping Interval</b>	The interval of the ICMP packet. Values range from 0 second to 30 seconds.
<b>Egress Interface (only for IPv6)</b>	<p>The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes.</p> <p>The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.</p> <p>When the egress interface is not given, PING6 finds the best match interface for destination.</p>

	<p>Do not specify egress interface for loopback address.</p> <p>Do specify egress interface for link-local or multicast address.</p>
--	--

Buttons	
	Click to start transmitting ICMP packets.
	Click to re-start diagnostics with PING.

## VeriPHY

Start

Press **Start** to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters.

10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

Start

After pressing **Start**, following table show up.

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	OK	189	OK	189	Open	0	Open	0
2	OK	3	OK	3	OK	3	OK	3
3	OK	189	OK	189	Open	0	Open	0
4	OK	189	OK	189	OK	189	Open	0
5	OK	189	OK	189	Cross A	48	Open	0
6	OK	189	OK	189	OK	189	Open	0

Object	Description
<b>Port</b>	The port where you are requesting VeriPHY Cable Diagnostics.
<b>Cable Status</b>	<p><b>Port:</b></p> <p>Port number.</p> <p><b>Pair:</b></p>



	<p>The status of the cable pair.</p> <p>OK - Correctly terminated pair</p> <p>Open - Open pair</p> <p>Short - Shorted pair</p> <p>Short A - Cross-pair short to pair A</p> <p>Short B - Cross-pair short to pair B</p> <p>Short C - Cross-pair short to pair C</p> <p>Short D - Cross-pair short to pair D</p> <p>Cross A - Abnormal cross-pair coupling with pair A</p> <p>Cross B - Abnormal cross-pair coupling with pair B</p> <p>Cross C - Abnormal cross-pair coupling with pair C</p> <p>Cross D - Abnormal cross-pair coupling with pair D</p> <p><b>Length:</b></p> <p>The length (in meters) of the cable pair. The resolution is 3 meters</p>
--	--

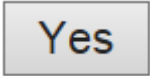
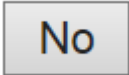
Buttons	
<div>Start</div>	Click to run the diagnostics.

# Maintenance

## Restart Device

You can restart the switch on this page. After restart, the switch will boot normally.

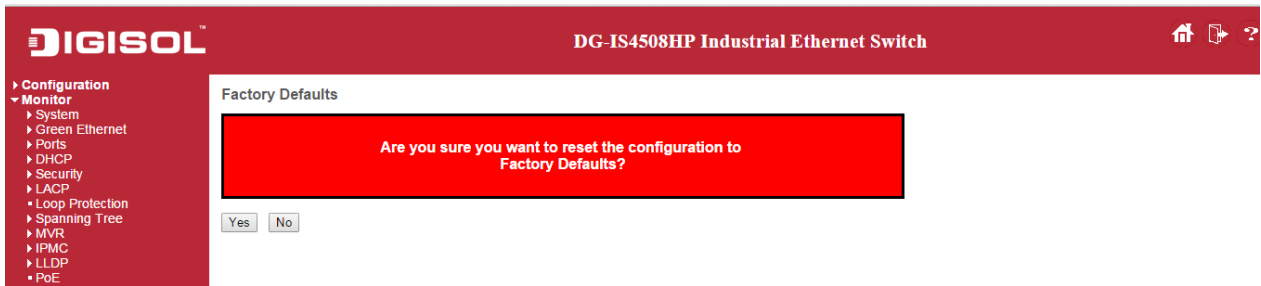


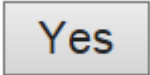
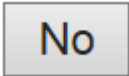
Buttons	
	Click to restart device.
	Click to return to the Port State page without restarting.

# Factory Default

You can reset the configuration of the switch on this page. Only the [IP](#) configuration is retained.

The new configuration is available immediately, which means that no restart is necessary.

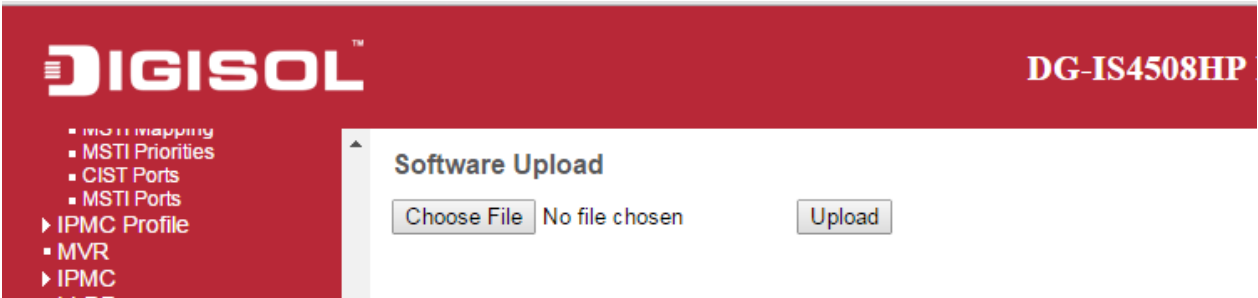


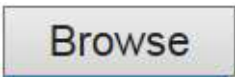

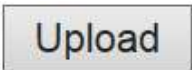
Buttons	
	Click to reset the configuration to Factory Defaults.
	Click to return to the Port State page without resetting the configuration.

# Software

## Software Upload

This page facilitates an update of the firmware controlling the switch.



Buttons	
	Go to find the software image and click  .
	After finding the software image, click the button to update firmware. After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.

**Warning:** While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. **Do not restart or power off the device at this time** or the switch may fail to function afterwards.

## Image select

This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.



The web page displays two tables with information about the active and alternate firmware images.

Note:

1. In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the **Activate Alternate Image** button is also disabled.
2. If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.



Object	Description
<b>Image</b>	The flash index name of the firmware image. The name of primary (preferred) image is <b>image</b> , the alternate image is named <b>image.bk</b> .
<b>Version</b>	The version of the firmware image.
<b>Data</b>	The date where the firmware was produced.

Buttons	
	Click to use the alternate image. This button may be disabled depending on system state.
	Cancel activating the backup image. Navigates away from this page.

## Configuration

### Save startup-config

Copy *running-config* to *startup-config*, thereby ensuring that the currently active configuration will be used at the next reboot.



## Download

It is possible to download any of the files on the switch to the web browser. Select the file and click

**Download Configuration**

Download *running-config* may take a little while to complete, as the file must be prepared for download.

The screenshot shows the DIGISOL web interface for the DG-IS4508HP switch. The interface has a red header with the DIGISOL logo on the left and the model number DG-IS4508HP on the right. A left sidebar contains a navigation menu with the following items: Configuration, Monitor, Diagnostics (with sub-items Ping, Ping6, and VeriPHY), Maintenance (with sub-items Restart Device, Factory Defaults, Software, and Configuration), and Configuration (with sub-items Save startup-config and Download). The main content area is titled 'Download Configuration' and contains the text 'Select configuration file to save.' and a note: 'Please note: running-config may take a while to prepare for download.' Below this is a table with the header 'File Name' and three rows: 'running-config', 'default-config', and 'startup-config', each with a radio button. At the bottom of the main content area is a 'Download Configuration' button.

**DIGISOL™** **DG-IS4508HP**

- Configuration
- Monitor
- ▼ Diagnostics
  - Ping
  - Ping6
  - VeriPHY
- ▼ Maintenance
  - Restart Device
  - Factory Defaults
  - ▼ Software
    - Upload
    - Image Select
  - ▼ Configuration
    - Save startup-config
    - Download

### Download Configuration

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

File Name
<input type="radio"/> running-config
<input type="radio"/> default-config
<input type="radio"/> startup-config

**Download Configuration**



## Upload

It is possible to upload a file from the web browser to all the files on the switch, except *default-config*, which is read-only.


Select the file to upload, select the destination file on the target, then click

**Upload Configuration**

If the destination is *running-config*, the file will be applied to the switch configuration. This can be done in two ways:

- Replace mode: The current configuration is fully replaced with the configuration in the uploaded file.
- Merge mode: The uploaded file is merged into *running-config*.

If the file system is full (i.e. contains the three system files mentioned above plus two other files), it is not possible to create new files, but an existing file must be overwritten or another deleted first.



**DG-IS4508HP**

- ▶ Configuration
- ▶ Monitor
- ▼ Diagnostics
  - Ping
  - Ping6
  - VeriPHY
- ▼ Maintenance
  - Restart Device
  - Factory Defaults
  - ▼ Software
    - Upload
    - Image Select
  - ▼ Configuration
    - Save startup-config
    - Download
    - Upload
    - Activate

### Upload Configuration

**File To Upload**

Choose File

 No file chosen

**Destination File**

File Name	Parameters
<input type="radio"/> running-config	<input checked="" type="radio"/> Replace <input type="radio"/> Merge
<input type="radio"/> startup-config	
<input type="radio"/> Create new file	<div style="border: 1px solid #ccc; height: 15px; width: 100%;"></div>

Upload Configuration

## Activate

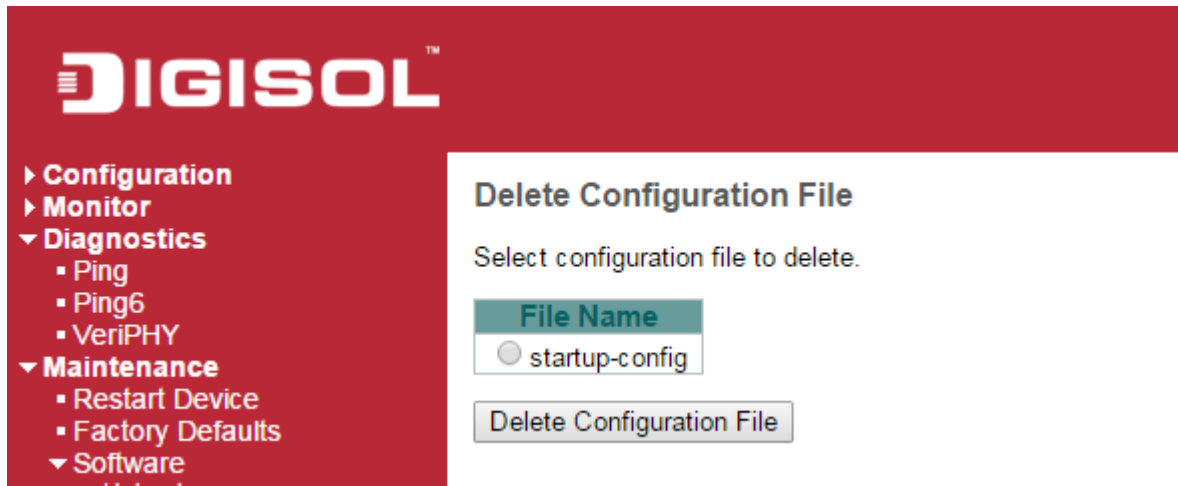
It is possible to activate any of the configuration files present on the switch, except for *running-config* which represents the currently active configuration.

Select the file to activate and click **Activate Configuration**. This will initiate the process of completely replacing the existing configuration with that of the selected file.



## Delete

It is possible to delete any of the writable files stored in flash, including *startup-config*. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to default configuration.



\* This product comes with Limited Life time warranty. For further details about warranty policy and Product Registration, please visit support section of [www.digisol.com](http://www.digisol.com)