



SISGM1040-184D-LRT

12-Port Managed Industrial Ethernet Switch

TRANSITION NETWORKS SISGM1040-184D-LRT

Open All / Close All

- System Information
- Front Panel
- Configuration
- Monitor
- Diagnostics
- Maintenance

System Information

Auto-refresh Refresh

System	
Contact	
Name	
Location	
Hardware	
MAC Address	00-c0-f2-7a-ce-e3
Chip ID	VSC7425
Time	
System Date	2000-01-01T01:39:39+00:00
System Uptime	0d 01:39:41
Software	
Software Version	v1.00.01
Software Date	2017-02-16T21:52:37+08:00
Acknowledgments	Details

Close

Web User Guide

33710 Rev A

Safety Warnings and Cautions

These products are not intended for use in life support products where failure of a product could reasonably be expected to result in death or personal injury. Anyone using this product in such an application without express written consent of an officer of Transition Networks does so at their own risk, and agrees to fully indemnify Transition Networks for any damages that may result from such use or sale.



Attention: this product, like all electronic products, uses semiconductors that can be damaged by ESD (electrostatic discharge). Always observe appropriate precautions when handling.



Note: Emphasizes important information or calls your attention to related features or instructions.



Warning: Alerts you to a potential hazard that could cause personal injury.



Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

SISGM1040-184D-LRT Web User Guide - TN PN 33710 Rev. A

Record of Revisions

Rev	Date	Description of Changes
A	3/14/17	Initial release for software v1.00.

Trademark notice: All trademarks and registered trademarks are the property of their respective owners. All other products or service names used in this publication are for identification purposes only, and may be trademarks or registered trademarks of their respective companies. All other trademarks or registered trademarks mentioned herein are the property of their respective holders.

Copyright restrictions: © 2017 Transition Networks, Inc. All rights reserved. No part of this work may be reproduced or used in any form or by any means (graphic, electronic, or mechanical) without written permission from Transition Networks.

Address comments on this product or manual to:

Transition Networks Inc.

10900 Red Circle Drive, Minnetonka, MN 55343

tel: +1.952.941.7600 | toll free: 1.800.526.9267 | fax: 952.941.2322

sales@transition.com | techsupport@transition.com | customerservice@transition.com

CONTENTS

1. Introduction.....	10
1.1 System Description.....	10
1.2 Using the Web Interface.....	10
1.2.1.1 Web Browser Support.....	10
1.2.1.2 System Navigation	11
1.2.1.3 Title Bar Icons	11
1.2.1.4 Ending a Session	12
1.2.1.5 Resetting to Factory Defaults.....	12
1.3 Related Manuals.....	12
2. Using the Web UI	13
2.1 Login	13
2.2 Tree View (Menu System)	13
2.3 Configuration.....	14
2.3.1.1 System.....	14
2.3.1.2 System Information.....	14
2.3.1.3 System IP.....	15
2.3.1.4 System NTP	18
2.3.1.5 System Time.....	19
2.3.1.6 System Log	22
2.3.1.7 System Alarm Profile.....	23
Green Ethernet.....	24
2.3.1.8 Port Power Savings	24
2.3.1.9 Ports.....	26
2.3.1.10 DHCP	28
2.3.1.11 DHCP Server	28
2.3.1.12 DHCP Server Mode	28
2.3.1.13 DHCP Server Excluded IP	30
2.3.1.14 DHCP Server Pool.....	31
2.3.1.15 DHCP Snooping	32
2.3.1.16 DHCP Relay.....	33
2.3.1.17 Security	35
2.3.1.18 Switch.....	35
2.3.1.19 Users	35
2.3.1.20 Privilege Level	37
2.3.1.21 Auth Method	39

2.3.1.22 SSH	40
2.3.1.23 HTTPS.....	41
2.3.1.24 Access Management.....	42
2.3.1.25 SNMP	44
2.3.1.26 SNMP System Configuration	44
2.3.1.27 SNMP Trap Configuration	46
2.3.1.28 SNMP Communities.....	51
2.3.1.29 SNMP Users	52
2.3.1.30 SNMP Groups.....	54
2.3.1.31 SNMP Views.....	55
2.3.1.32 SNMP Access.....	56
2.3.1.33 RMON	58
2.3.1.34 RMON Statistics	58
2.3.1.35 RMON History.....	59
2.3.1.36 RMON Alarm.....	60
2.3.1.37 RMON Event	62
2.3.1.38 Network	63
2.3.1.39 Limit Control	63
2.3.1.40 NAS	66
2.3.1.41 ACL	76
2.3.1.42 ACL Port	76
2.3.1.43 ACL Rate Limiters	78
2.3.1.44 Access Control List	79
2.3.1.45 IP Source Guard	91
2.3.1.46 IP Source Guard Configuration	91
2.3.1.47 IP Source Guard Static Table	93
2.3.1.48 ARP Inspection.....	94
2.3.1.49 Port Configuration	94
2.3.1.50 VLAN Mode Configuration	96
2.3.1.51 Static ARP Inspection Table.....	97
2.3.1.52 Dynamic ARP Inspection Table	98
2.3.1.53 AAA	100
2.3.1.54 RADIUS.....	100
2.3.1.55 TACACS+	102
2.3.1.56 Aggregation.....	104
2.3.1.57 Static Aggregation.....	104
2.3.1.58 LACP Aggregation.....	106
2.3.1.59 Loop Protection	108
2.3.1.60 Spanning Tree	110

2.3.1.61 Bridge Settings	110
2.3.1.62 MSTI Mapping.....	112
2.3.1.63 MSTI Priorities.....	114
2.3.1.64 CIST Ports	115
2.3.1.65 MSTI Ports.....	117
2.3.1.66 IPMC Profile	119
2.3.1.67 Profile Table	119
2.3.1.68 Address Entry.....	121
2.3.1.69 MVR	122
2.3.1.70 IPMC.....	125
2.3.1.71 IGMP Snooping	125
2.3.1.72 Basic Configuration	125
2.3.1.73 VLAN Configuration	127
2.3.1.74 Port Filtering Profile.....	129
2.3.1.75 MLD Snooping.....	130
2.3.1.76 Basic Configuration	130
2.3.1.77 VLAN Configuration	132
2.3.1.78 Port Filtering Profile.....	134
2.3.1.79 LLDP	135
2.3.1.80 LLDP	135
2.3.1.81 LLDP-MED	138
2.3.1.82 MAC Table.....	144
2.3.1.83 VLANs.....	146
2.3.1.84 Private VLANs.....	150
2.3.1.85 Membership.....	150
2.3.1.86 Port Isolation.....	152
2.3.1.87 VCL	153
2.3.1.88 MAC-based VLAN.....	153
2.3.1.89 Protocol-based VLAN	155
2.3.1.90 Protocol to Group	155
2.3.1.91 Group to VLAN	157
2.3.1.92 IP Subnet-based VLAN	159
2.3.1.93 Voice VLAN.....	161
2.3.1.94 Voice VLAN Configuration.....	161
2.3.1.95 Voice VLAN OUI.....	163
2.3.1.96 QoS.....	164
2.3.1.97 Port Classification	164
2.3.1.98 Port Policing.....	166

- 2.3.1.99 Port Scheduler 167
- 2.3.1.100 Port Shaping 169
- 2.3.1.101 Port Tag Remarking 170
- 2.3.1.102 Port DSCP 171
- 2.3.1.103 DSCP-Based QoS..... 173
- 2.3.1.104 DSCP Translation 174
- 2.3.1.105 DSCP Classification 175
- 2.3.1.106 QoS Control List..... 176
- 2.3.1.107 Storm Control 180
- 2.3.1.108 Mirror 181
- 2.3.1.109 GVRP..... 183
- 2.3.1.110 GVRP Global Config 183
- 2.3.1.111 GVRP Port Config..... 184
- 2.3.1.112 sFlow 185
- 2.3.1.113 Redundant Ring & Chain Configuration 188
- 2.3.1.114 DDMI Configuration 195
- 2.4 Monitor 196
 - 2.4.1.1 System..... 196
 - 2.4.1.2 System Information..... 196
 - 2.4.1.3 CPU Load..... 197
 - 2.4.1.4 IP Status 198
 - 2.4.1.5 System Log 200
 - 2.4.1.6 Detailed System Log..... 202
 - 2.4.1.7 System Alarm 203
 - 2.4.1.9 Green Ethernet 205
 - 2.4.1.10 Port Power Savings Data 205
 - 2.4.1.11 Ports 206
 - 2.4.1.12 Ports State Overview 206
 - 2.4.1.13 Traffic Overview 206
 - 2.4.1.14 QoS Statistics 208
 - 2.4.1.15 QCL Status..... 209
 - 2.4.1.16 Detailed Statistics..... 211
 - 2.4.1.17 DHCP 213
 - 2.4.1.18 DHCP Server 213
 - 2.4.1.19 Statistics 213
 - 2.4.1.20 Binding 215
 - 2.4.1.21 Declined IP 216
 - 2.4.1.22 DHCP Snooping Table..... 217
 - 2.4.1.23 DHCP Relay Statistics 219

2.4.1.24 DHCP Detailed Statistics	221
2.4.1.25 Security	223
2.4.1.26 Access Management Statistics.....	223
2.4.1.27 Network	224
2.4.1.28 Port Security	224
2.4.1.29 Switch.....	224
2.4.1.30 Port	227
2.4.1.31 NAS	229
2.4.1.32 Switch.....	229
2.4.1.33 Port	230
2.4.1.34 ACL Status	233
2.4.1.35 ARP Inspection.....	235
2.4.1.36 IP Source Guard	237
2.4.1.37 AAA	238
2.4.1.38 RADIUS Overview.....	238
2.4.1.39 RADIUS Details.....	240
2.4.1.40 Switch.....	241
2.4.1.41 RMON	241
2.4.1.42 Statistics.....	241
2.4.1.43 History.....	243
2.4.1.44 Alarm	245
2.4.1.45 Event	246
2.4.1.46 LACP	247
2.4.1.47 System Status.....	247
2.4.1.48 Port Status	248
2.4.1.49 Port Statistics	249
2.4.1.50 Loop Protection	250
2.4.1.51 Spanning Tree	251
2.4.1.52 Bridge Status.....	251
2.4.1.53 Port Status	253
2.4.1.54 Port Statistics	254
2.4.1.55 MVR	255
2.4.1.56 MVR Statistics	255
2.4.1.57 MVR Channel Groups.....	256
2.4.1.58 MVR SFM Information	257
2.4.1.59 IPMC.....	259
2.4.1.60 IGMP Snooping	259
2.4.1.61 IGMP Snooping Status	259

- 2.4.1.62 Groups Information 261
- 2.4.1.63 IPv4 SFM Information 262
- 2.4.1.64 MLD Snooping..... 264
- 2.4.1.65 MLD Snooping Status..... 264
- 2.4.1.66 Groups Information 266
- 2.4.1.67 IPv6 SFM Information 267
- 2.4.1.68 LLDP 269
- 2.4.1.69 Neighbors..... 269
- 2.4.1.70 LLDP-MED Neighbors 271
- 2.4.1.71 EEE 276
- 2.4.1.72 Port Statistics 278
- 2.4.1.73 MAC Table 280
- 2.4.1.74 VLANs..... 282
- 2.4.1.75 VLANs Membership 282
- 2.4.1.76 VLANs Ports..... 284
- 2.4.1.77 VCL 286
- 2.4.1.78 MAC-Based VLAN..... 286
- 2.4.1.79 sFlow 287
- 2.4.1.80 Redundant Ring & Chain Monitoring..... 289
- 2.4.1.81 DDMI Monitoring..... 291
- 2.4.1.82 Overview..... 291
- 2.4.1.83 Detailed..... 292
- 2.5 Diagnostics 293
 - 2.5.1.1 Ping 293
 - 2.5.1.2 Ping6 295
 - 2.5.1.3 VeriPHY 297
- 2.6 Maintenance 299
 - 2.6.1.1 Restart Device 299
 - 2.6.1.2 Factory Default..... 300
 - 2.6.1.3 Software..... 301
 - 2.6.1.4 Software Upload 301
 - 2.6.1.5 Image Select..... 302
 - 2.6.1.6 Configuration 303
 - 2.6.1.7 Save startup-config 303
 - 2.6.1.8 Download Configuration..... 304
 - 2.6.1.9 Upload Configuration..... 305
 - 2.6.1.10 Activate Configuration 306
 - 2.6.1.11 Delete Configuration File 307

3. Technical Specifications 308

4. Service, Warranty, and Tech Support..... 312

5. Compliance Information..... 312

Glossary..... 313

1. Introduction

1.1 System Description

Transition Networks' SISGM1040-184D-LRT industrial Ethernet switch delivers high quality, wide operating temperature range, extended power input range, IP-30 design, and advanced VLAN and QoS features. This switch is 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.

The SISGM1040-184D-LRT eases the effort to build a network infrastructure which offers reliable, well managed and high quality networking for any business requiring continuous and well-protected services in management environments. With features such as Fast Failover ring protection and QoS, customers can ensure their network is qualified to deliver real-time high quality applications.

1.2 Using the Web Interface

This manual addresses the features, design, layout and operation of the web UI.

1.2.1.1 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

1.2.1.2 System Navigation

All of the Web UI main screens can be viewed by clicking on hyperlinks in the four menu boxes on the left side of the screen: Configuration, Monitor, Diagnostics, and Maintenance.

1.2.1.3 Title Bar Icons

The Web UI startup screen (the System Information page) is shown below.

The screenshot shows the 'System Information' page for a Transition Networks device. The page includes a sidebar with navigation options, a main content area with system details, and a right sidebar with a port status diagram.

System Information

System	
Contact Name	
Contact Location	
Hardware	
MAC Address	00-c0-f2-7a-ce-e3
Chip ID	VSC7425
Time	
System Date	2000-01-01T01:39:39+00:00
System Uptime	0d 01:39:41
Software	
Software Version	v1.00.01
Software Date	2017-02-16T21:52:37+08:00
Acknowledgments	Details

Auto-refresh Refresh

12-Port Managed Industrial Ethernet Switch

Close

Show Help Button



Each screen has a Help button that displays 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. For more information about any screen, click on the Help button on the screen; help information is displayed in a new window.

Logout Button



Click the Logout button to display a webpage message confirming that you want to logout of the web site. Click the **OK** button to confirm that you want to logout, or click the Cancel button to remain logged in.

When you log out, the Login page displays again.

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 CLI), a Save icon displays 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 displays.
2. Click on **Submit** next to Data Control Action drop-down list on top of System/Save and Restore screen.

The **Save** button on each page only saves the config in RAM; always remember to save the config in flash once all the changes are done.

1.2.1.4 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.

1.2.1.5 Resetting to Factory Defaults

Note that only the **telnet** interface is capable of bringing back the factory default IP address.

The factory default IP address would be retained after defaulting via the Web UI. To bring back factory defaults, use the commands below:

```
# reload defaults (including reload the default IP address)
or
# reload defaults keep-ip (reload factory defaults, but keep the current IP address)
# copy running-config startup-config
```

See the *CLI Reference* for additional information.

1.3 Related Manuals

These manuals give additional information on how to operate the switch:

- SISGM1040-184D-LRT Quick Start Guide, 33708
- SISGM1040-184D-LRT Install Guide, 33709
- SISGM1040-184D-LRT CLI Reference, 33711

For Transition Networks Drivers, Firmware, Manual, etc. go to the [Product Support](#) webpage (logon required).

For Transition Networks Application Notes, Brochures, Data Sheets, Specifications, etc. go to the [Support Library](#) (no logon required). Note that this manual provides links to third party web sites for which Transition Networks is not responsible.

2. Using the Web UI

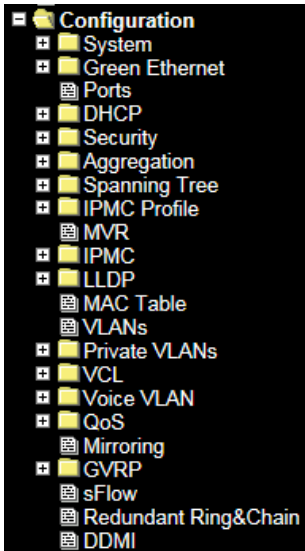
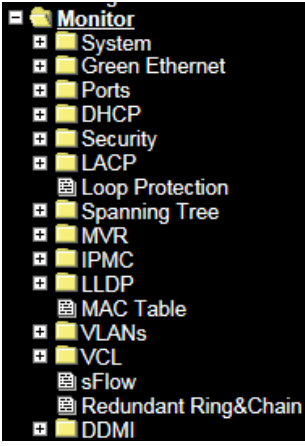
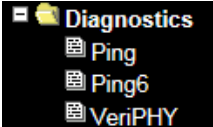
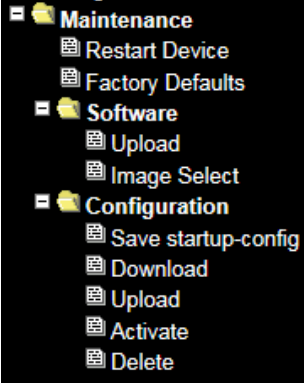
2.1 Login

See the SISGM1040-184D-LRT Install Guide for installation details.

Operation	1. Enter Username and Password. 2. Click "Sign in".
Field	Description
Username	Login user name. The maximum length is 32. Default: root
Password	Login user password. The maximum length is 32. Default: root

2.2 Tree View (Menu System)

The tree view provides the Web UI menu system. It lets you quickly to get to the desired page for Configuration, Monitoring, Diagnostics, or Maintenance.

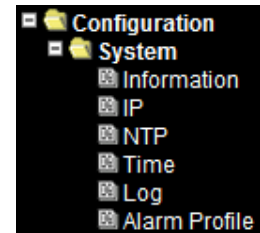
 <ul style="list-style-type: none"> [-] Configuration <ul style="list-style-type: none"> [+] System [+] Green Ethernet Ports [+] DHCP [+] Security [+] Aggregation [+] Spanning Tree [+] IPMC Profile MVR [+] IPMC [+] LLDP <ul style="list-style-type: none"> MAC Table VLANs [+] Private VLANs [+] VCL [+] Voice VLAN [+] QoS Mirroring [+] GVRP sFlow Redundant Ring&Chain DDMI 	 <ul style="list-style-type: none"> [-] Monitor <ul style="list-style-type: none"> [+] System [+] Green Ethernet Ports [+] DHCP [+] Security [+] LACP Loop Protection [+] Spanning Tree [+] MVR [+] IPMC [+] LLDP <ul style="list-style-type: none"> MAC Table VLANs [+] VCL sFlow Redundant Ring&Chain [+] DDMI 	 <ul style="list-style-type: none"> [-] Diagnostics <ul style="list-style-type: none"> Ping Ping6 VeriPHY 	 <ul style="list-style-type: none"> [-] Maintenance <ul style="list-style-type: none"> Restart Device Factory Defaults [-] Software <ul style="list-style-type: none"> Upload Image Select [-] Configuration <ul style="list-style-type: none"> Save startup-config Download Upload Activate Delete
Configuration menu	Monitor menu	Diagnostics menu	Maintenance menu

Each of the Web UI main menus is described in the following sections.

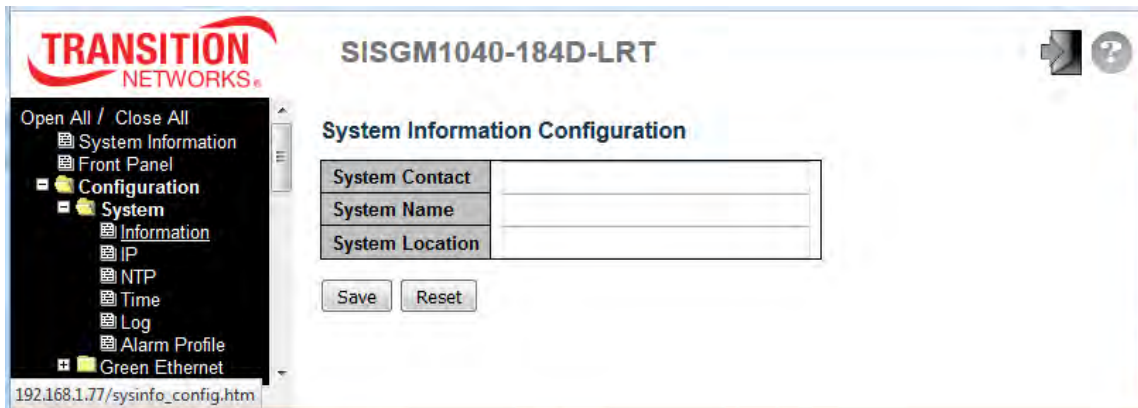
2.3 Configuration

2.3.1.1 System

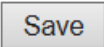

2.3.1.2 System Information



Configure the switch system information here.

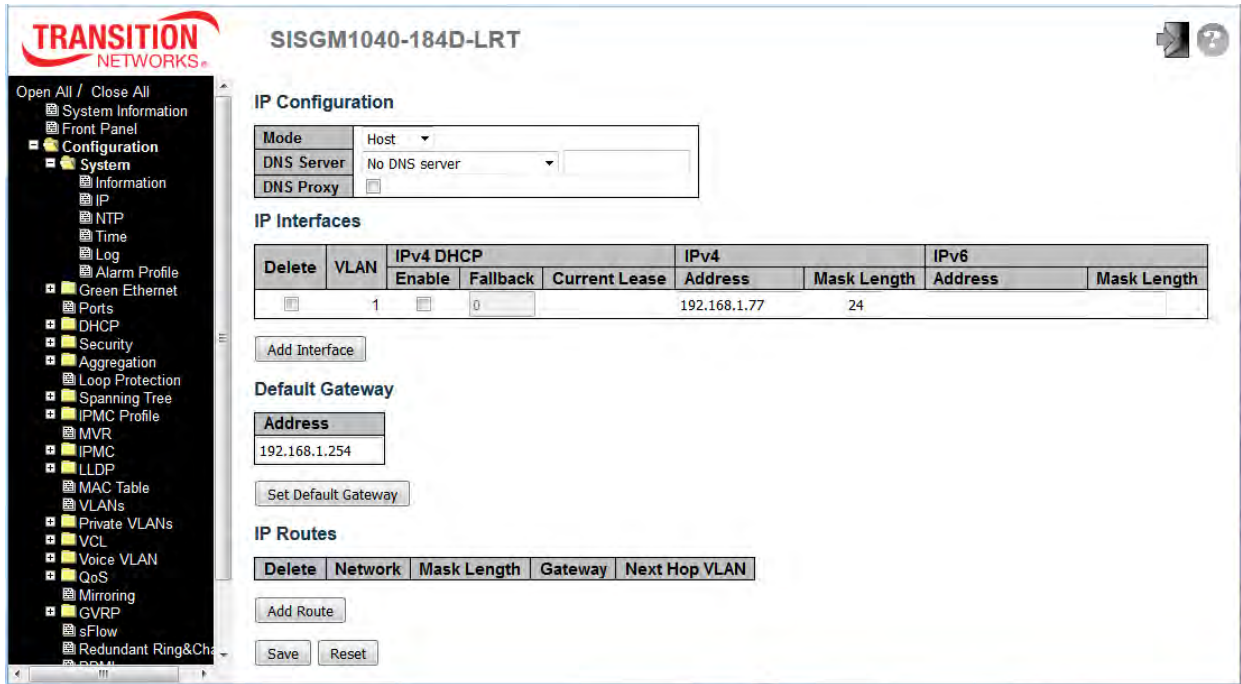


Object	Description
System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
System Name	An administratively assigned 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.
System Location	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 immediately.
	Click to revert to previously saved values.

2.3.1.3 System IP

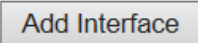
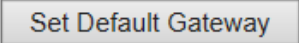
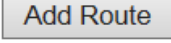
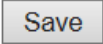
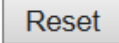
Configure IP basic settings, control IP interfaces and IP routes here. Up to eight interfaces and up to 32 routes are supported.



Object	Description
IP Configuration	
Mode	Configure whether the IP stack should act as a Host or a Router . In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces.
DNS Server	This setting controls the DNS name resolution done by the switch. The following modes are supported: From any DHCP interfaces : The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used. No DNS server : No DNS server will be used. Configured : Explicitly provide the IP address of the DNS Server in dotted decimal notation. From this DHCP interface : Specify from which DHCP-enabled interface a provided DNS server should be preferred.

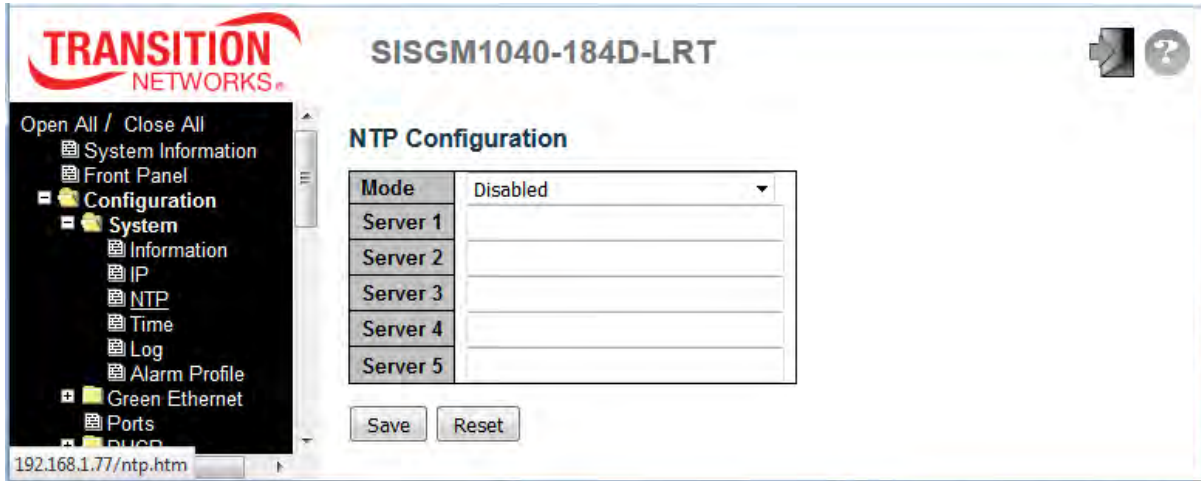
DNS Proxy	When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network.
IP Interfaces	
Delete	Select this option to delete an existing IP interface.
VLAN	The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.
IPv4 DHCP Enabled	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.
IPv4 DHCP Fallback Timeout	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.
IPv4 DHCP Current Lease	For DHCP interfaces with an active lease, this column show the current interface address, as provided by the DHCP server.
IPv4 Address	The IPv4 address of the interface in dotted decimal notation. If DHCP 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.
IPv4 Mask	The IPv4 network mask, in number of bits (<i>prefix length</i>). Valid values are between 0 and 30 bits for an IPv4 address. If DHCP 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.
IPv6 Address	The IPv6 address of the interface. An 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, <code>fe80::215:c5ff:fe03:4dc7</code> . The symbol <code>::</code> 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, <code>::192.1.2.34</code> . The field may be left blank if IPv6 operation on the interface is not desired.
IPv6 Mask	The IPv6 network mask, in number of bits (<i>prefix length</i>). Valid values are between 1 and 128 bits for an IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.

Default Gateway	
Address	The IP address of the gateway valid format is dotted decimal notation (e.g., 192.168.1.254).
IP Routes	
Delete	Select this option to delete an existing IP route.
Network	The destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value <code>0.0.0.0</code> or IPv6 <code>::</code> notation.
Mask Length	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 <code>0</code> (as it will match anything).
Gateway	The IP address of the IP gateway. Valid format is dotted decimal notation or a valid IPv6 notation. Gateway and Network must be of the same type.
Next Hop VLAN (Only for IPv6)	<p>The VLAN ID (VID) of the specific IPv6 interface associated with the gateway.</p> <p>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>

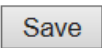

Buttons	
	Click to add a new IP interface. A maximum of 8 interfaces is supported.
	Click to save changes.
	Click to add a new IP route. A maximum of 32 routes is supported.
	Click to save changes immediately.
	Click to revert to previously saved values.

2.3.1.4 System NTP

Configure NTP (Network Timing Protocol) on this page.



Object	Description
Mode	Indicates the NTP mode operation. Possible modes are: Enabled: Enable NTP client mode operation. Disabled: Disable NTP client mode operation.
Server #	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.

2.3.1.5 System Time

This page lets you configure the Time Zone and Daylight Savings Time (DST) from the **Configuration > System > NTP** menu path.

The screenshot shows the web interface for SISGM1040-184D-LRT. On the left is a navigation tree with categories like System Information, Front Panel, Configuration, System, Information, IP, NTP, Time, Log, Alarm Profile, Green Ethernet, Ports, DHCP, Security, Aggregation, Loop Protection, Spanning Tree, IPMC Profile, MVR, IPMC, LLDP, MAC Table, VLANs, Private VLANs, VCL, Voice VLAN, QoS, Mirroring, GVRP, sFlow, Redundant Ring&Chain, DDMI, Monitor, Diagnostics, and Maintenance. The main content area is titled 'Time Zone Configuration' and contains three sections:

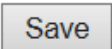

- Time Zone Configuration:** A table with 'Time Zone' set to 'None' and 'Acronym' set to '(0 - 16 characters)'.
- Daylight Saving Time Configuration:** A table with 'Daylight Saving Time' set to 'Disabled'. Below it are 'Start Time settings' and 'End Time settings' tables, both with Month: Jan, Date: 1, Year: 2000, Hours: 0, and Minutes: 0.
- Offset settings:** A table with 'Offset' set to '1 (1 - 1440) Minutes'.
- Date/Time Configuration:** A table with 'Year' set to '2000 (2000 - 2037)', 'Month' set to 'Jan', 'Date' set to '1', 'Hours' set to '1', 'Minutes' set to '58', and 'Seconds' set to '9'.

At the bottom of the configuration area are 'Save' and 'Reset' buttons.

Object	Description
Time Zone Configuration	
Time Zone	Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Save to set.
Acronym	User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range : 0 to 16 characters)

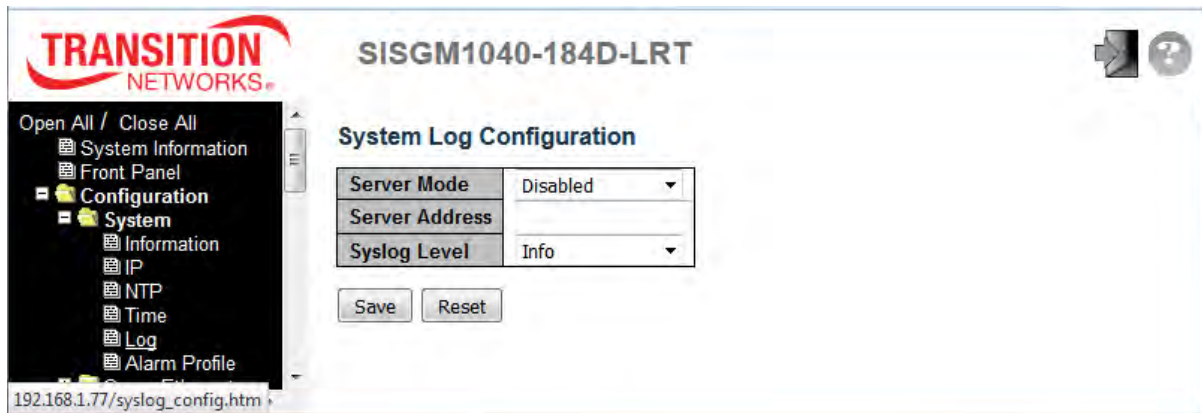
Daylight Saving Time Configuration	
Daylight Saving Time	This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight 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)
Recurring Configurations	
Start time settings	
Week	Select the starting week number.
Day	Select the starting day.
Month	Select the starting month.
Hours	Select the starting hour.
Minutes	Select the starting minute
End time settings	
Week	Select the ending week number.
Day	Select the ending day.
Month	Select the ending month.
Hours	Select the ending hour.
Minutes	Select the ending minute
Offset settings	
Offset	Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)
Non Recurring Configurations	
Start time settings	
Month	Select the starting month.
Date	Select the starting date.
Year	Select the starting year.
Hours	Select the starting hour.
Minutes	Select the starting minute
End time settings	
Month	Select the ending month.
Date	Select the ending date.
Year	Select the ending year (2000 - 2037).
Hours	Select the ending hour. (0-23)

Minutes	Select the ending minute (0-59).
Seconds	Select the ending second (0-59).
Offset settings	
Offset	Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)
Date/Time Configuration	
Date/Time Settings	
Year	Current year of date/time (range: 2000 to 2037).
Month	Current month of current date/time.
Date	Current date of current date/time.
Hours	Current hour of current date/time.
Minutes	Current minute of current date/time.
Seconds	Current second of current date/time.

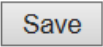

Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

2.3.1.6 System Log

Configure System Logging (SysLog) on this page.



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

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

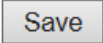
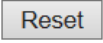
2.3.1.7 System Alarm Profile

The Alarm Profile table is provided here to enable/disable the alarm. **Note:** When any alarm exists, the Alarm LED will be on (lit); the Alarm Output Relay will also be enabled.

The screenshot shows the 'Alarm Profile' configuration page. The table below is a representation of the data shown in the interface.

ID	Description	Enabled
*	*	<input type="checkbox"/>
1	Port 1 Link Down	<input type="checkbox"/>
2	Port 2 Link Down	<input type="checkbox"/>
3	Port 3 Link Down	<input type="checkbox"/>
4	Port 4 Link Down	<input type="checkbox"/>
5	Port 5 Link Down	<input type="checkbox"/>
6	Port 6 Link Down	<input type="checkbox"/>
7	Port 7 Link Down	<input type="checkbox"/>
8	Port 8 Link Down	<input type="checkbox"/>
9	Port 9 Link Down	<input type="checkbox"/>
10	Port 10 Link Down	<input type="checkbox"/>
11	Port 11 Link Down	<input type="checkbox"/>
12	Port 12 Link Down	<input type="checkbox"/>
13	Power Alarm	<input type="checkbox"/>

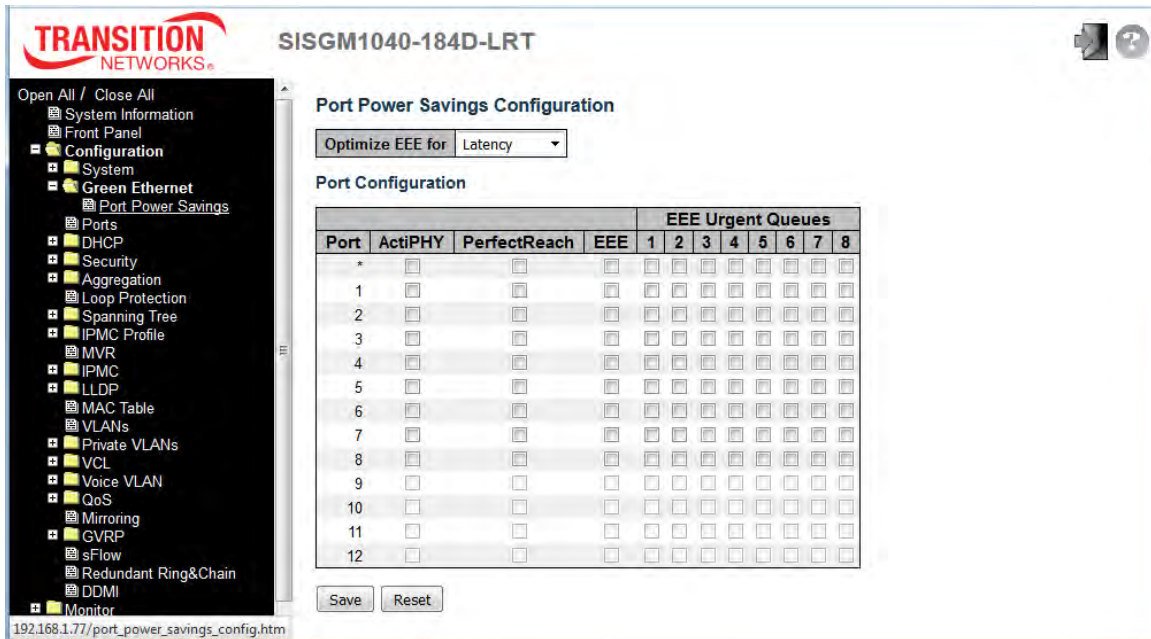
Object	Description
ID	The identification number of the Alarm Profile entry. Note that the top row has an ID of * which indicates this as a “select all” function.
Description	A description of the Alarm Type (e.g., Port x Link Down, Power Alarm).
Enabled	If alarm entry is Enabled, then alarm will be shown in alarm history/current when it occurs. The Alarm LED will be on (lit), The Alarm Relay will also be enabled. An SNMP trap will be sent if any SNMP trap entry exists and is enabled.
Disabled	If alarm entry is Disabled, then alarm will not be captured/shown in alarm history/current when alarm occurs; then it will not trigger the Alarm LED change, Alarm Relay or SNMP trap.

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

Green Ethernet

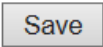
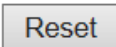
2.3.1.8 Port Power Savings

This page lets you configure copper port power savings features.



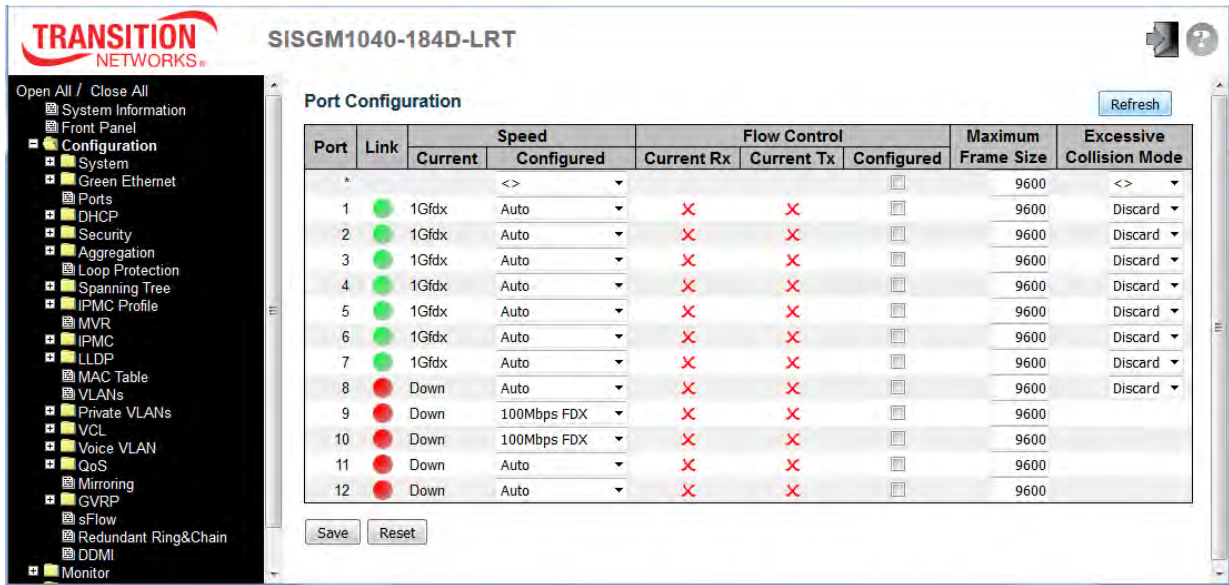
Object	Description
Port Power Savings Configuration	
Optimize EEE for	The switch can be set to optimize EEE for either best power saving or least traffic latency.
Port Configuration	
Port	The switch port number of the logical port. Note that the top row has an ID of * which indicates this as a “select all” function.
ActiPHY	Link down power savings enabled. 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.
PerfectReach	Cable length power savings enabled. PerfectReach works by determining the cable length and lowering the power for ports with short cables.
EEE	Controls whether Energy Efficient Ethernet is enabled for this copper port. For maximizing power savings, the circuit isn't started the instant 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.

	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.
EEE Urgent Queues	Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

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

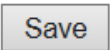

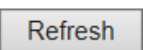
2.3.1.9 Ports

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



Object	Description
Port	This is the logical port number for this row. Note that the top row has an ID of * which indicates this as a “select all” function.
Link	The current link state is displayed graphically. Green indicates the link is up and red that it is down.
Current Link Speed	Provides the current link speed of the port.
Configured Link Speed	<p>Selects any available link speed for the given switch port. Only speeds supported by the specific port are shown. Possible speeds are:</p> <ul style="list-style-type: none"> Disabled - Disables the switch port operation. Auto - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner. 10Mbps HDX - Forces the cu port in 10Mbps half-duplex mode. 10Mbps FDX - Forces the cu port in 10Mbps full duplex mode. 100Mbps HDX - Forces the cu port in 100Mbps half-duplex mode. 100Mbps FDX - Forces the cu port in 100Mbps full duplex mode. 1Gbps FDX - Forces the port in 1Gbps full duplex.

Flow Control	<p>When Auto Speed is selected on a port, this section indicates the flow control 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 Auto-Negotiation.</p> <p>Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.</p>
Maximum Frame Size	Enter the maximum frame size allowed for the switch port, including FCS.
Excessive Collision Mode	<p>Configure port transmit collision behavior.</p> <p>Discard: Discard frame after 16 collisions (default).</p> <p>Restart: 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 immediately. Any changes made locally will be undone.

2.3.1.10 DHCP

DHCP (Dynamic Host Configuration Protocol) is used for assigning dynamic IP addresses to devices on a network. DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

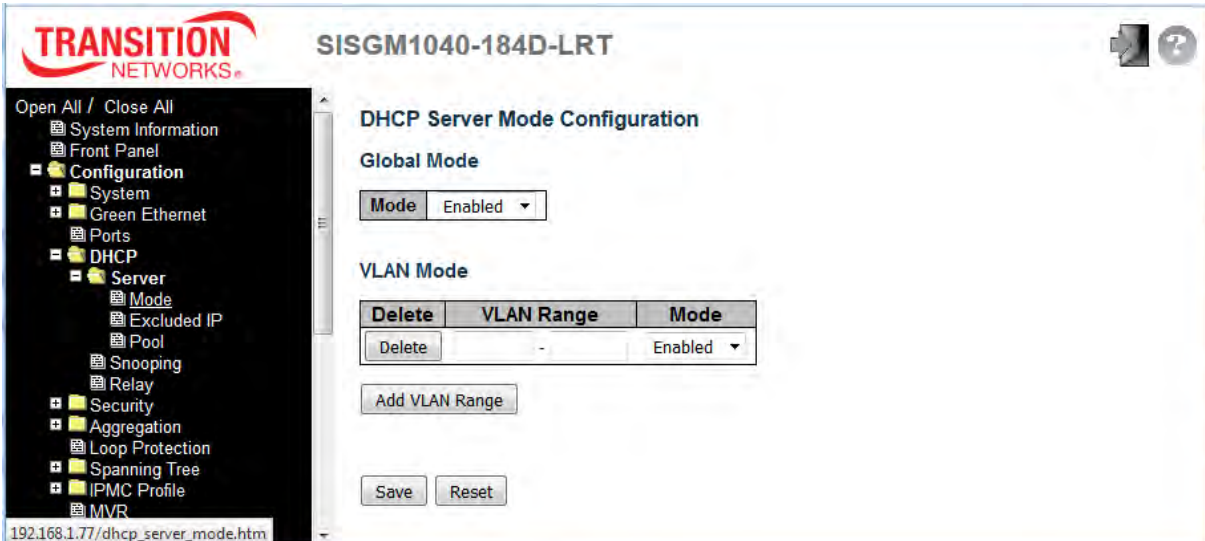
Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

2.3.1.11 DHCP Server

A DHCP Server is used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP client.

2.3.1.12 DHCP Server Mode

This page configures global mode and VLAN mode to enable/disable DHCP server per system and per VLAN. Click the **Add New VLAN Range** button to enable VLAN Mode and add a new VLAN range.



The screenshot displays the web interface for configuring the DHCP Server Mode. The page title is "SISGM1040-184D-LRT" and the main heading is "DHCP Server Mode Configuration".

Global Mode

Mode: Enabled

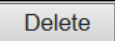
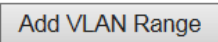
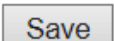
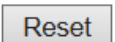
VLAN Mode

Delete	VLAN Range	Mode
Delete	-	Enabled

Buttons: Add VLAN Range, Save, Reset

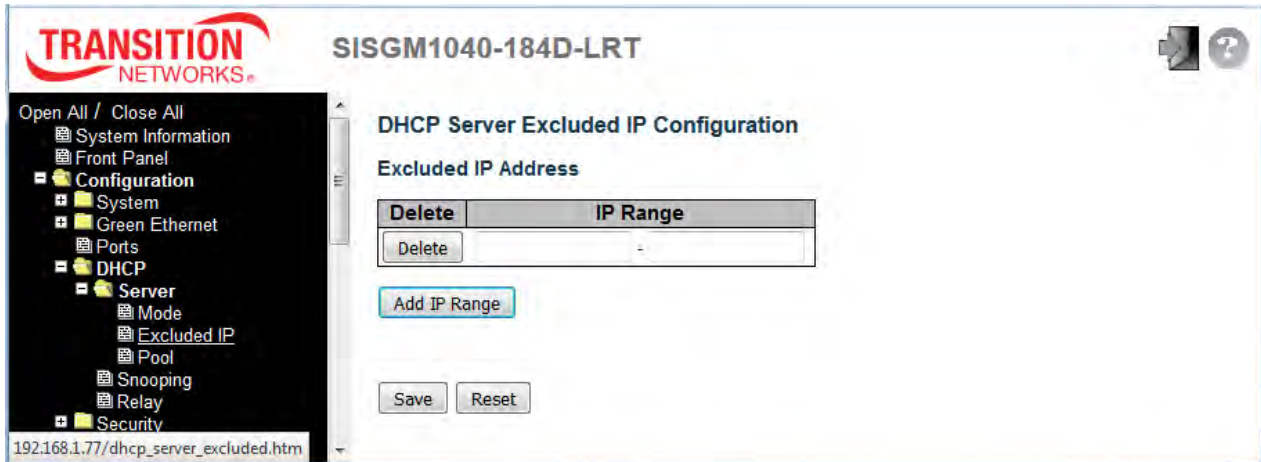
Navigation menu (left): Open All / Close All, System Information, Front Panel, Configuration (System, Green Ethernet, Ports, DHCP, Server, Mode, Excluded IP, Pool, Snooping, Relay, Security, Aggregation, Loop Protection, Spanning Tree, IPMC Profile, MVR), 192.168.1.77/dhcp_server_mode.htm

Object	Description
Global Mode	
Mode	Configure the operation mode per system. Possible modes are: Enabled: Enable DHCP server per system. Disabled: Disable DHCP server per system.
VLAN Mode	
VLAN Range	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. <u>BUT</u> , if the VLAN range contains only one VLAN ID, then you can just enter it into either one of the first and second VLAN ID or both. On the other hand, if you want to disable existing VLAN range, follow these steps. <ol style="list-style-type: none"> 1. Press the Add VLAN Range button to add a new VLAN range. 2. Input the VLAN range that you want to disable. 3. Choose Mode to be Disabled. 4. Press the Save button to apply the change. You will see that the disabled VLAN range is removed from the DHCP Server mode configuration page.
Mode	Indicate the operation mode per VLAN. Possible modes are: Enabled: Enable DHCP server per VLAN. Disabled: Disable DHCP server pre VLAN.

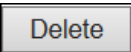

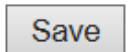
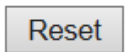
Buttons	
	Click to delete the setting.
	Click to add a new VLAN range.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

2.3.1.13 DHCP Server Excluded IP

This page configures excluded IP addresses. DHCP server will not allocate these excluded IP addresses to DHCP client. Click the **Add New IP Range** button to add a new IP range.

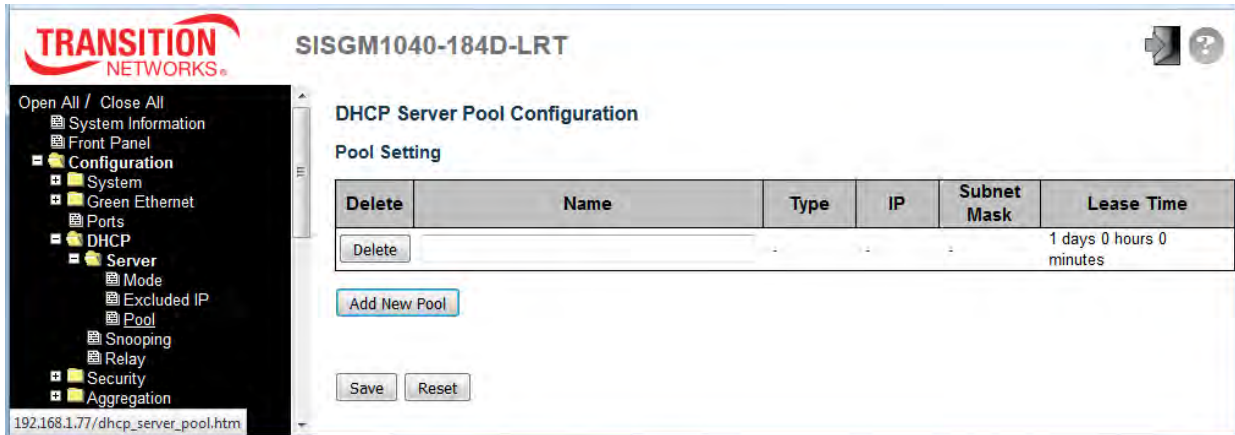


Object	Description
IP Range	Define the IP range to be excluded IP addresses. The first excluded IP must be smaller than or equal to the second excluded IP. BUT, if the IP range contains only 1 excluded IP, then you can just input it to either one of the first and second excluded IPs or both.

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.

2.3.1.14 DHCP Server Pool

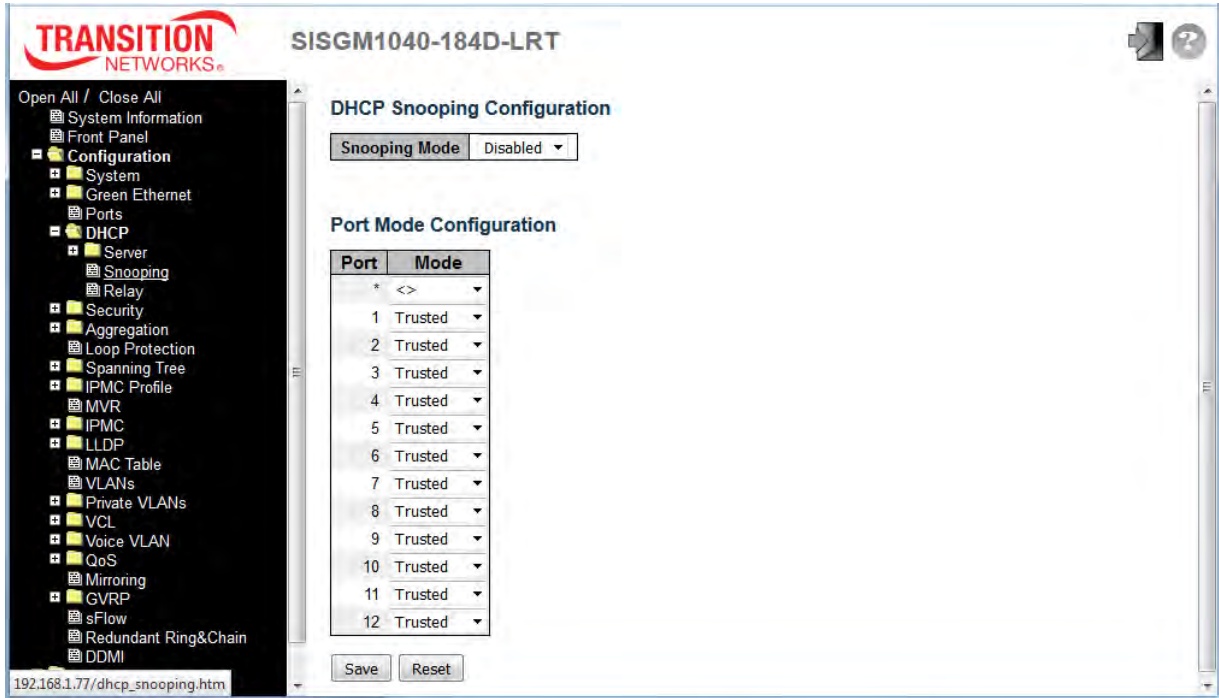
This page manages DHCP pools. According to the DHCP pool, DHCP server will allocate IP address and deliver configuration parameters to DHCP client.



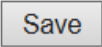

Object	Description
Name	Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page.
Type	Display which type the pool is: Network : the pool defines a pool of IP addresses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

2.3.1.15 DHCP Snooping

Configure DHCP Snooping on this page.



Object	Description
Snooping Mode	Indicates the DHCP snooping mode of operation. Possible modes are: Enabled: 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. Disabled: Disable DHCP snooping mode operation.
Port Mode Configuration	Indicates the DHCP snooping port mode. Possible port modes are: Trusted: Configures the port as trusted source of the DHCP messages. Untrusted: 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.



2.3.1.16 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
Relay Mode	<p>Indicates the DHCP relay mode operation.</p> <p>Possible modes are:</p> <p>Enabled: 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>Disabled: Disable DHCP relay mode operation.</p>
Relay Server	<p>Indicates the DHCP relay server IP address.</p>
Relay Information Mode	<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), and the last two characters are the port number. For example, "00030108" means the DHCP message received from VLAN ID 3, switch ID 1, port 8, and the option 82 remote ID value is equal to the switch MAC address.</p> <p>Possible modes are:</p> <p>Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option</p>

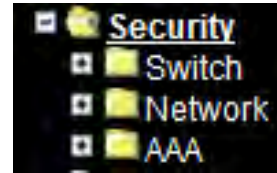
	<p>82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.</p> <p>Disabled: Disable DHCP relay information mode operation.</p>
<p>Relay Information Policy</p>	<p>Indicates the 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>Replace: Replace the original relay information when a DHCP message that already contains it is received.</p> <p>Keep: Keep the original relay information when a DHCP message that already contains it is received.</p> <p>Drop: Drop the package when a DHCP message that already contains relay information is received.</p>

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

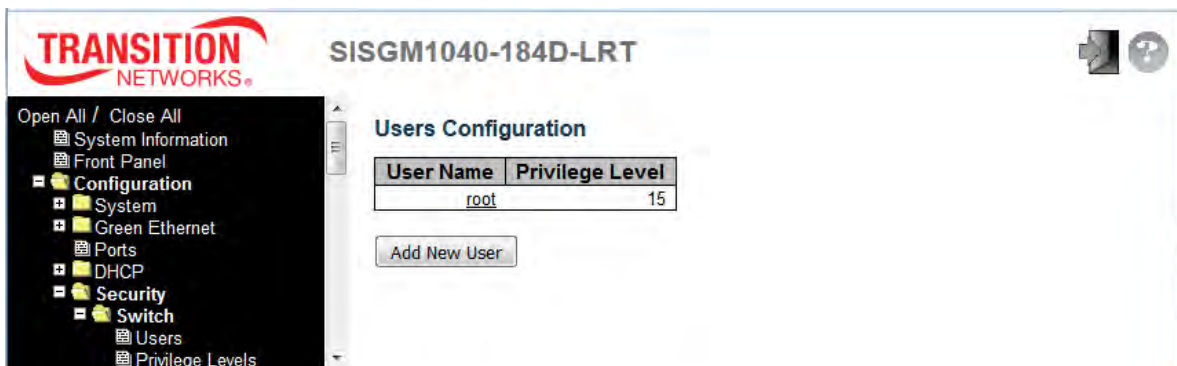
2.3.1.17 Security

2.3.1.18 Switch

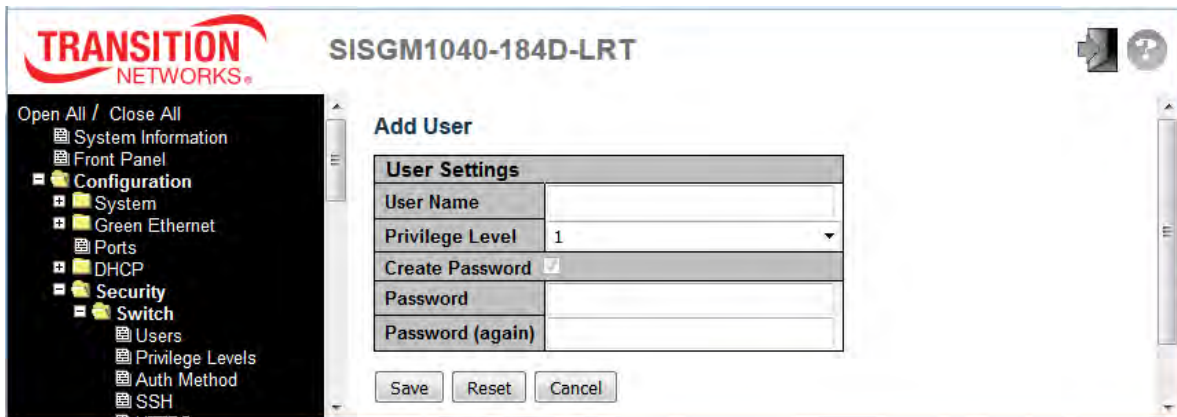
2.3.1.19 Users



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 default User config is shown below.


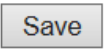
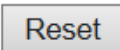
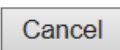
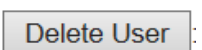


You can click the linked default User to edit its parameters, or click the **Add New User** button to add and configure one or more new users.



Object	Description
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 31. The valid user name allows letters, numbers and underscores.
Password	The password of the user. The allowed string length is 0 to 31. Any printable character including space is accepted.

Privilege Level	The privilege level of the user. The allowed range is 1 to 15 . If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But other values 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, most groups' privilege level 5 has the read-only access and privilege level 10 has read-write access. System maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, 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).

2.3.1.20 Privilege Level

This page provides an overview of the privilege levels.

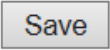
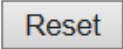
Privilege Level Configuration

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
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

Save Reset

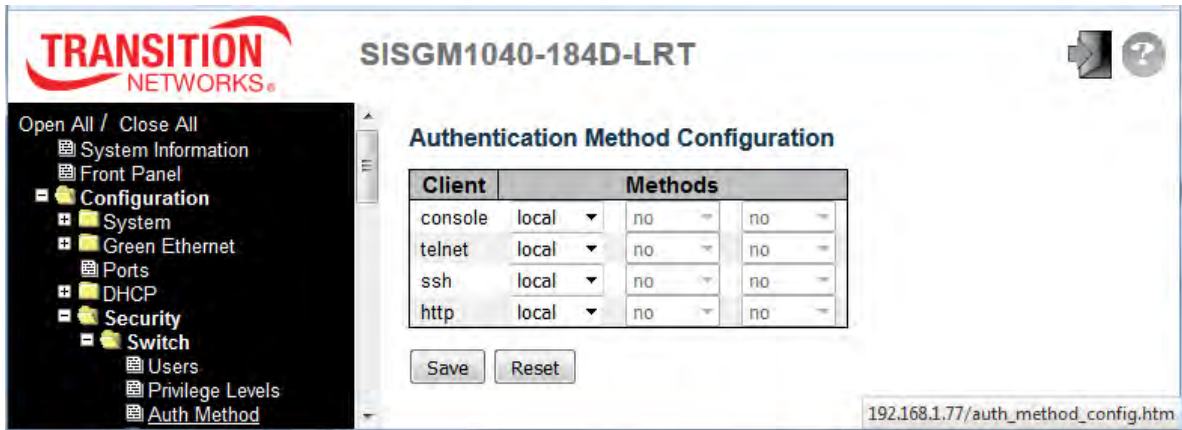
Object	Description
Group Name	<p>The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details:</p> <p>System: Contact,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

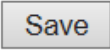
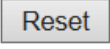
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

2.3.1.21 Auth Method

This page lets you configure how a user is authenticated when they log into the switch via one of the management client interfaces.



Object	Description
Client	The management client for which the configuration below applies (console, telnet, ssh, http).
Methods	<p>Method can be set to one of these values:</p> <ul style="list-style-type: none"> no: Authentication is disabled and login is not possible. local: Use the local user database on the switch for authentication. radius: Use remote RADIUS server(s) for authentication. tacacs+: Use remote TACACS+ server(s) for authentication. <p>Methods that involve 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.

2.3.1.22 SSH

Configure SSH (Secure Shell) on this page. SSH provides a secure channel over an unsecured network in a client-server architecture, connecting an SSH client application with an SSH server.



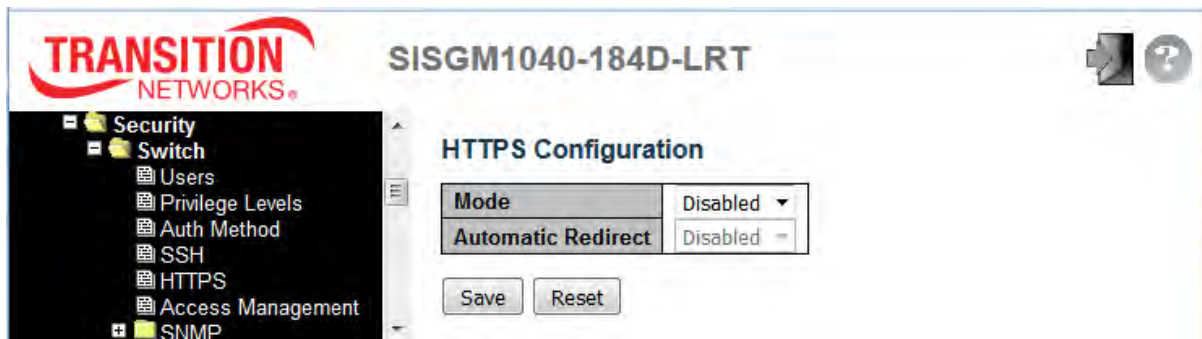
Object	Description
Mode	Indicates the SSH mode operation. Possible modes are: Enabled: Enable SSH mode operation (default). Disabled: Disable SSH mode operation.

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


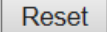
2.3.1.23 HTTPS

Configure HTTPS (secure HTTP) on this page. A message like *"The webpage at https://192.168.1.77/ might be temporarily down or it may have moved permanently to a new web address."* displays.

Your browser session closes and you must log in again at <https://192.168.1.77>. If a message such as *"Your connection is not private"* displays, click the **Advanced** button, and then select **Proceed to 192.168.1.77 (unsafe)**. You can then log back in using your current User Name and Password.



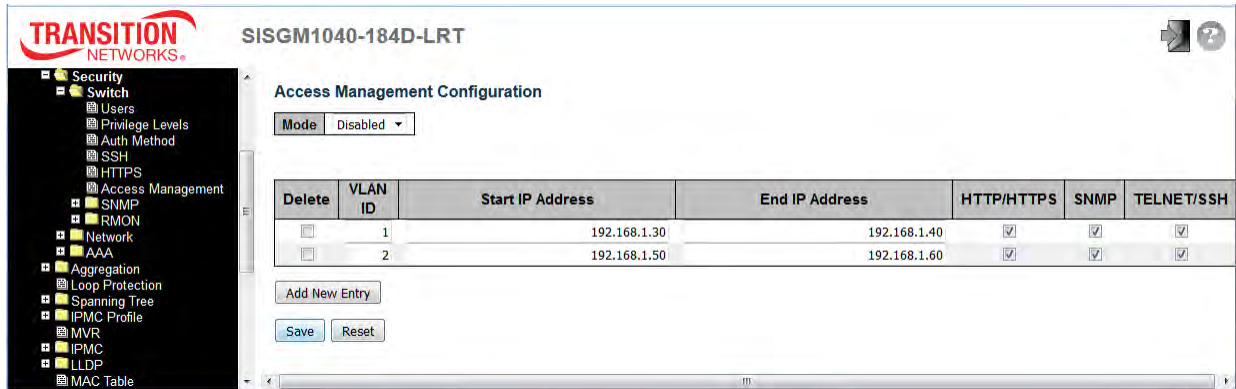
Object	Description
Mode	Sets / shows the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. Possible modes are: Enabled: Enable HTTPS mode operation. Disabled: Disable HTTPS mode operation (default).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

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




2.3.1.24 Access Management

Configure access management table on this page. The maximum number of entries is **16**.

If an application's type matches any one of the access management entries, it will allow access to the switch. At least one Allowed Access must be selected for each row. The entry content cannot be duplicated (two instances can not have the same IP address range assigned).

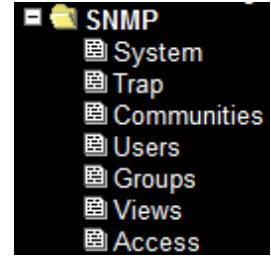


Object	Description
Mode	Indicates the access management mode operation. Possible modes are: Enabled : Enable access management mode operation. Disabled : Disable access management mode operation.
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	Indicates the VLAN ID for the access management entry.
Start IP Address	Indicates the starting IP address for the access management entry.
End IP Address	Indicates the ending IP address for the access management entry.
HTTP/HTTPS	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.
SNMP	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.
TELNET/SSH	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.

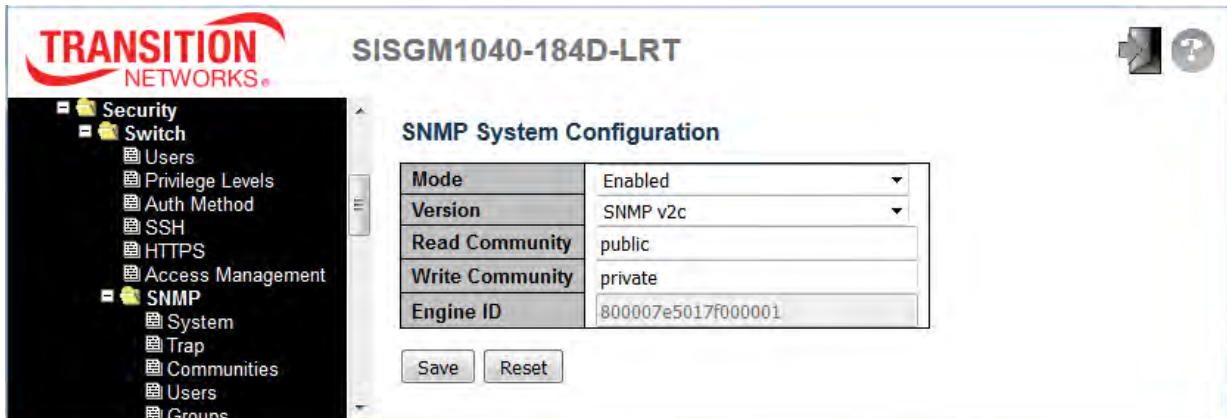
Buttons	
	Click to add a new access management entry.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

2.3.1.25 SNMP

2.3.1.26 SNMP System Configuration

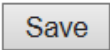
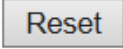


Configure SNMP on this page.



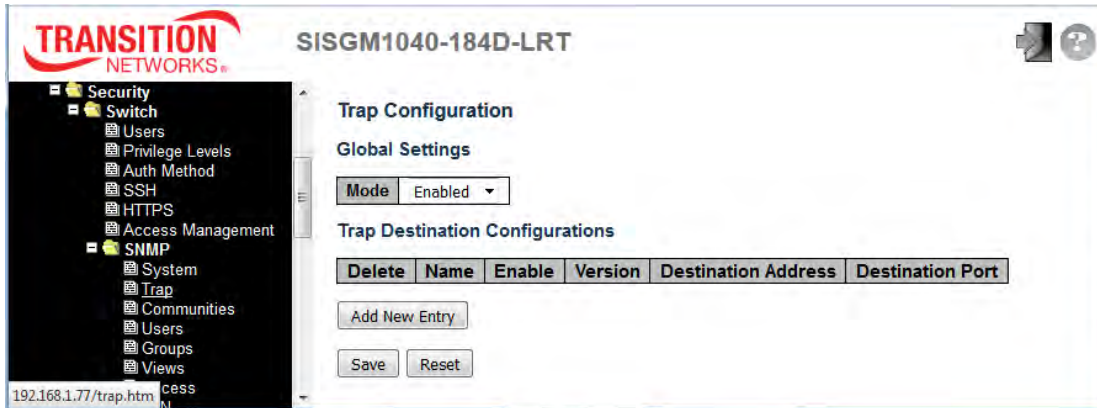
Object	Description
Mode	Indicates the SNMP mode operation. Possible modes are: Enabled: Enable SNMP mode operation. Disabled: Disable SNMP mode operation.
Version	Indicates the SNMP supported version. Possible versions are: SNMP v1: Set SNMP supported version 1. SNMP v2c: Set SNMP supported version 2c. SNMP v3: Set SNMP supported version 3.
Read Community	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.
Write Community	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. 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.
Engine ID	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.

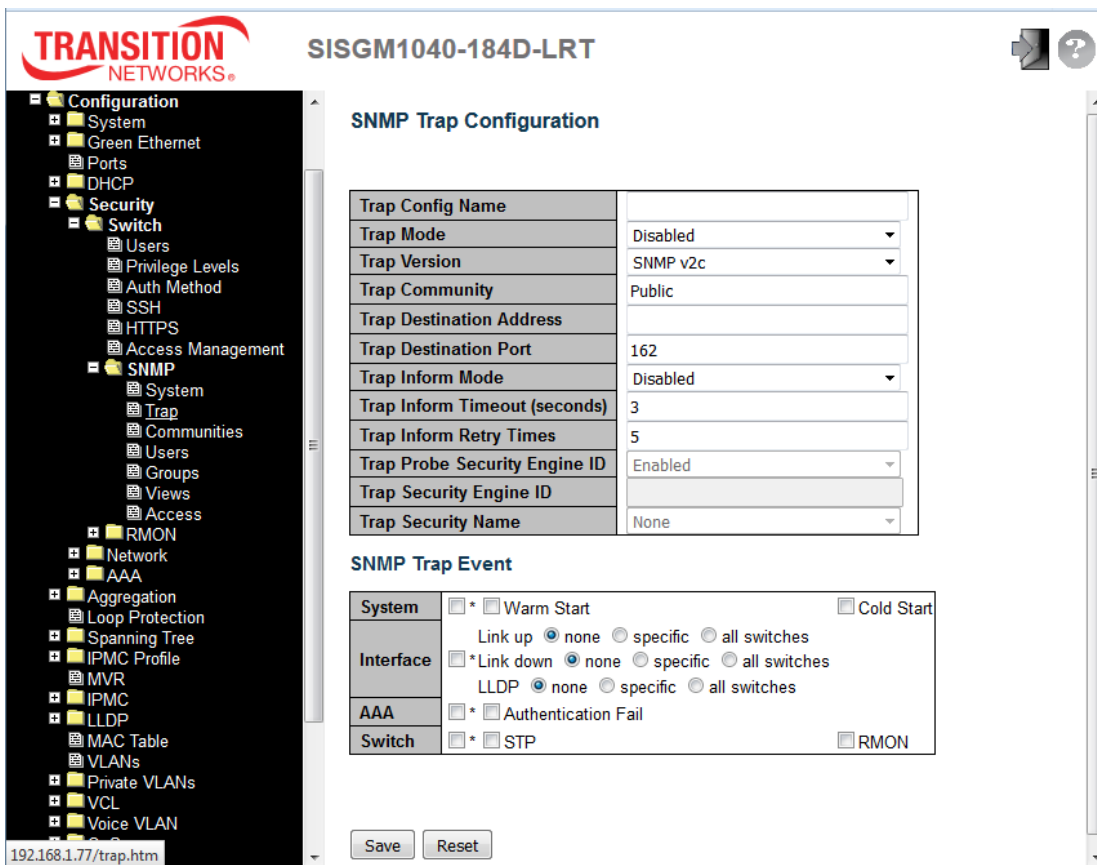
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

2.3.1.27 SNMP Trap Configuration

To configure SNMP traps, navigate to the Configuration > Security > Switch > SNMP > Trap menu path and at the Mode dropdown select **Enabled**.



Click the **Add New Entry** button to display the SNMP Trap Configuration page.



Configure SNMP traps on this page. The SNMP trap parameters are described below.

Object	Description
Global Settings	
Mode	<p>Indicates the trap mode operation. Possible modes are:</p> <p>Enabled: Enable SNMP trap mode operation.</p> <p>Disabled: Disable SNMP trap mode operation.</p>
Trap Destination Configurations	
Name	Indicates the trap Configuration's name. Indicates the trap destination's name.
Enable	<p>Indicates the trap destination mode operation. Possible modes are:</p> <p>Enabled: Enable SNMP trap mode operation.</p> <p>Disabled: Disable SNMP trap mode operation.</p>
Version	<p>Indicates the SNMP trap supported version. Possible versions are:</p> <p>SNMPv1: Set SNMP trap supported version 1.</p> <p>SNMPv2c: Set SNMP trap supported version 2c.</p> <p>SNMPv3: Set SNMP trap supported version 3.</p>
Destination Address	<p>Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). It also allows 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>
Destination port	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

The SNMP Trap Configuration table includes these fields (SNMP v2c on the left, SNMP v3 on the right):

SNMP Trap Configuration		SNMP Trap Configuration	
Trap Config Name	<input type="text"/>	Trap Config Name	<input type="text"/>
Trap Mode	Disabled	Trap Mode	Disabled
Trap Version	SNMP v2c	Trap Version	SNMP v3
Trap Community	Public	Trap Community	Public
Trap Destination Address	<input type="text"/>	Trap Destination Address	<input type="text"/>
Trap Destination Port	162	Trap Destination Port	162
Trap Inform Mode	Disabled	Trap Inform Mode	Disabled
Trap Inform Timeout (seconds)	3	Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5	Trap Inform Retry Times	5
Trap Probe Security Engine ID	Enabled	Trap Probe Security Engine ID	Enabled
Trap Security Engine ID	<input type="text"/>	Trap Security Engine ID	Probe Fail
Trap Security Name	None	Trap Security Name	None

Object	Description
Trap Config Name	Enter a name for the SNMP Trap configuration (optional).
Trap Mode	Indicates the SNMP trap mode operation. Possible modes are: Enabled : Enable SNMP trap mode operation. Disabled : Disable SNMP trap mode operation.
Trap Version	Indicates the SNMP trap supported version. Possible versions are: SNMP v1 : Set SNMP trap supported version 1. SNMP v2c : Set SNMP trap supported version 2c. SNMP v3 : Set SNMP trap supported version 3.
Trap Community	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.
Trap Destination Address	Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w'). 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.
Trap Destination Port	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.
Trap Authentication Failure	Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible modes are: Enabled : Enable SNMP trap authentication failure. Disabled : Disable SNMP trap authentication failure.

Trap Link-up and Link-down	Indicates the SNMP trap link-up and link-down mode operation. Possible modes are: Enabled: Enable SNMP trap link-up and link-down mode operation. Disabled: Disable SNMP trap link-up and link-down mode operation.
Trap Inform Mode	Indicates the SNMP trap inform mode operation. Possible modes are: Enabled: Enable SNMP trap inform mode operation. Disabled: Disable SNMP trap inform mode operation.
Trap Inform Timeout (seconds)	Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147 .
Trap Inform Retry Times	Indicates the SNMP trap inform retry times. The allowed range is 0 to 255 .
Trap Probe Security Engine ID	Indicates the SNMP trap probe security engine ID mode of operation. Possible values are: Enabled: Enable SNMP trap probe security engine ID mode of operation. Disabled: Disable SNMP trap probe security engine ID mode of operation.
Trap Security Engine ID	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.
Trap Security Name	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.

SNMP Trap Events

The SNMP Trap Events table includes these fields:

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
	<input type="checkbox"/> * 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

Object	Description
System	Enable/disable the Interface group's traps. Possible traps are: Warm Start: Enable/disable Warm Start trap. Cold Start: Enable/disable Cold Start trap.
Interface	Sets the Interface group's traps. Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible traps are: Link Up: Enable/disable Link up trap for none / specific / all switches). Link Down: Enable/disable Link down trap for none / specific / all switches). LLDP: Enable/disable LLDP trap for none / specific / all switches).
AAA	Indicates that the AAA group's traps. Possible traps are: SNMP Authentication Fail : Enable/disable SNMP trap authentication failure trap.
Switch	Indicates that the Switch group's traps. Possible traps are: STP: Enable/disable STP trap. RMON: Enable/disable RMON trap.

Specific Trap Event Configuration: If you select the 'specific' radio button for the SNMP Trap Events 'Link up', 'Link down', and 'LLDP', the port-specific table displays. Configure the events on a per-port basis as required. Click the **Save** button when done.

Buttons	
<input type="button" value="Add New Entry"/>	Click to add and configure a new SNMP user.
<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.

2.3.1.28 SNMP Communities

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

Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Community	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.
Source IP	Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.
Source Mask	Indicates the SNMP access source address mask.



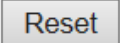
Buttons	
	Click to add a new community entry.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

2.3.1.29 SNMP Users

To configure SNMP users, navigate to the Configuration > Security > Switch > SNMP > Users menu path and click the **Add New Entry** button. Configure SNMPv3 user table on this page. The entry index keys are **Engine ID** and **User Name**.

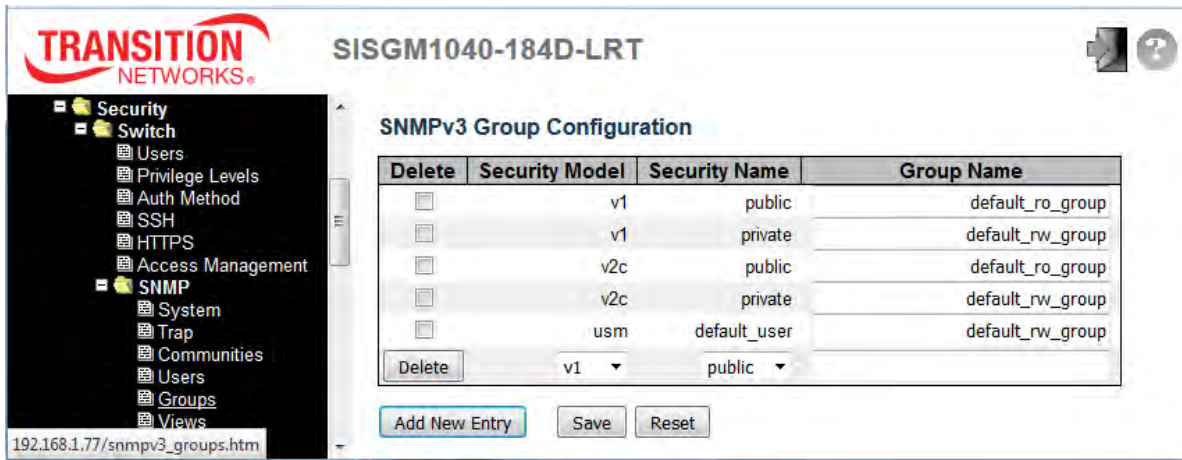
Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and 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 <i>usmUserEngineID</i> and <i>usmUserName</i> are the entry's keys. In a simple agent, <i>usmUserEngineID</i> is always that agent's own <i>snmpEngineID</i> value. The value can also take the value of the <i>snmpEngineID</i> of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equals system engine ID then it is local user; otherwise it's remote user.
User Name	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.
Modify Password	When you create a new entry, check the Modify Password checkbox (required). When password of entry is going to be changed, this option should also be checked; otherwise, the password will not be changed.
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv : No authentication and no privacy. Auth, NoPriv : Authentication and no privacy.

	<p>Auth, Priv: Authentication and privacy.</p> <p>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.</p>
Authentication Protocol	<p>Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:</p> <p>None: No authentication protocol.</p> <p>MD5: Indicates that this user uses MD5 (message-digest algorithm) authentication.</p> <p>SHA: Indicates that this user uses SHA (Secure Hash Algorithm) authentication.</p> <p>The value of security level cannot be modified if the entry already exists. This means you must first ensure that the value is set correctly.</p>
Authentication Password	<p>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.</p>
Privacy Protocol	<p>Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:</p> <p>None: No privacy protocol.</p> <p>DES: Indicate that this user uses DES (Data Encryption Standard) authentication protocol.</p> <p>AES: Indicate that this user uses AES (Advanced Encryption Standard) authentication protocol.</p>
Privacy Password	<p>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.</p>

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

2.3.1.30 SNMP Groups

Configure SNMPv3 group table on this page. The entry index keys are **Security Model** and **Security Name**. From the default page, click the **Add New Entry** button to add and configure a new SNMP group.

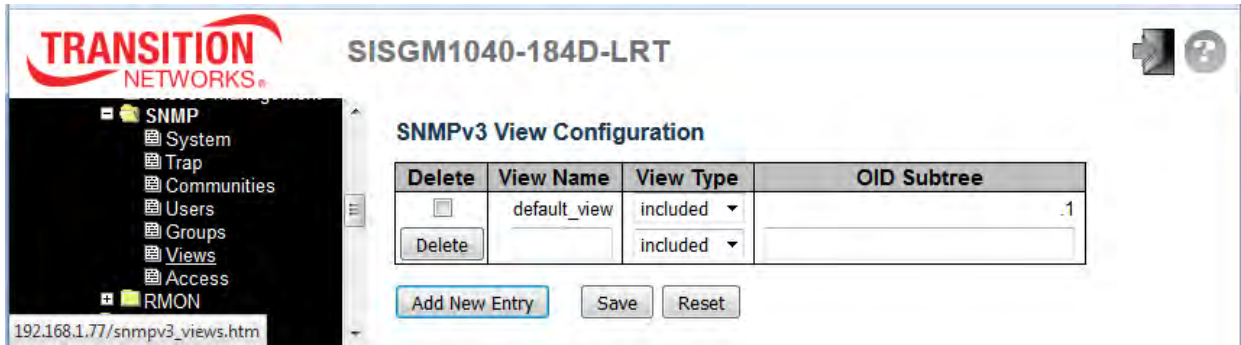


Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Security Model	Indicates the security model that this entry belongs to. Possible security models are: v1 : Reserved for SNMPv1. v2c : Reserved for SNMPv2c. usm : User-based Security Model (USM).
Security Name	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	
	Click to add a new group entry
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

2.3.1.31 SNMP Views

Configure SNMPv3 view table on this page. The entry index keys are **View Name** and **OID Subtree**. Click the **Add New Entry** button to add and configure a new SNMP View entry.

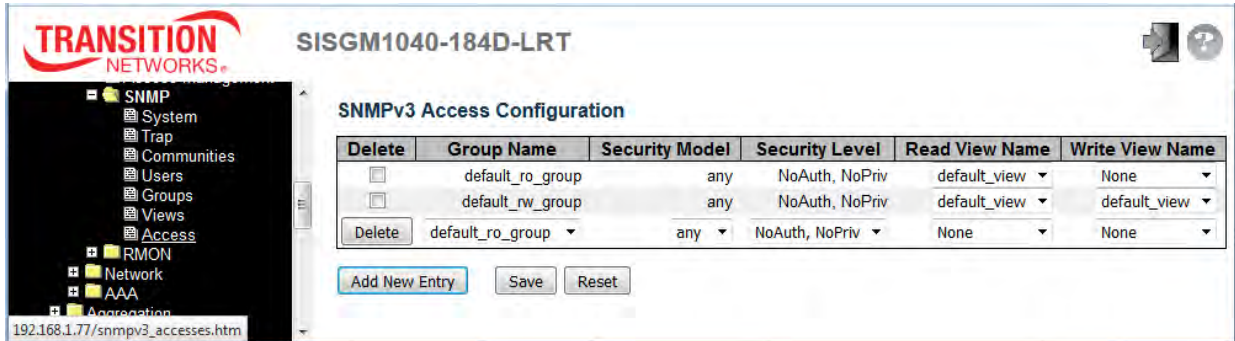


Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
View Type	Indicates the view type that this entry should belong to. Possible view types are: included : An optional flag to indicate that this view subtree should be included. excluded : 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 its OID subtree should overstep the 'excluded' view entry.
OID Subtree	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 (*).


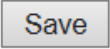
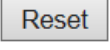
Buttons	
	Click to add a new SNMP View entry.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

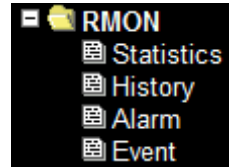
2.3.1.32 SNMP Access

Configure SNMPv3 Access values on this page. The entry index keys are **Group Name**, **Security Model** and **Security Level**. Click the **Add New Entry** button to add and configure a new SNMP Access entry.



Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
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.
Security Model	Indicates the security model that this entry should belong to. Valid security models are: any : Any security model accepted (v1 v2c usm). v1 : Reserved for SNMPv1. v2c : Reserved for SNMPv2c. usm : User-based Security Model (USM).
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv : No authentication and no privacy. Auth, NoPriv : Authentication and no privacy. Auth, Priv : Authentication and privacy.
Read View Name	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 - 32, and the allowed content is ASCII characters 33 - 126.
Write View Name	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.

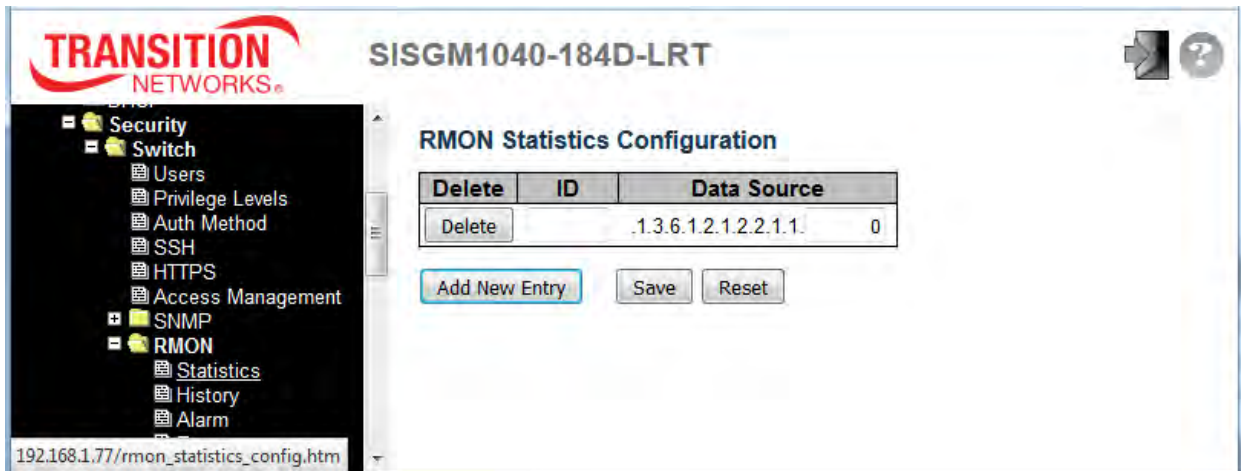
Buttons	
	Click to add a new access entry.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.



2.3.1.33 RMON

2.3.1.34 RMON Statistics

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



Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Data Source	Indicates the port ID which wants to be monitored.

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.

2.3.1.35 RMON History

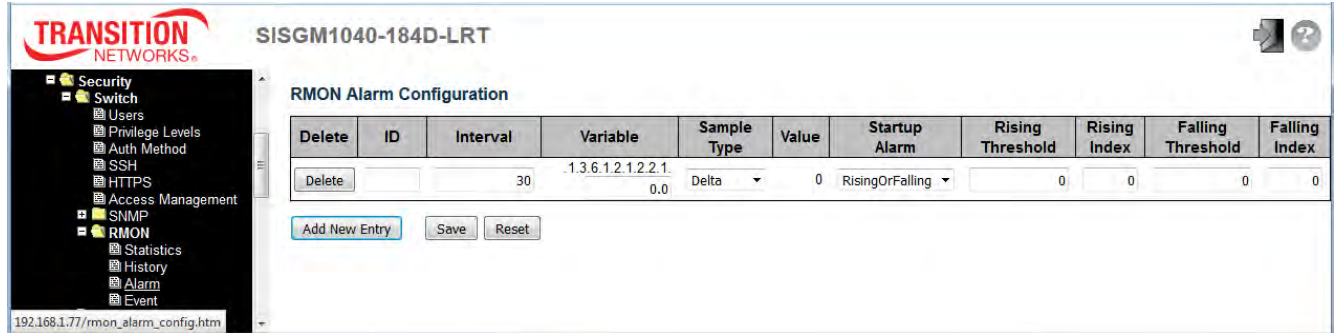
Configure the RMON History table on this page. The entry index key is **ID**.

Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The valid range is 1 - 65535.
Data Source	Indicates the port ID which wants to be monitored.
Interval	Indicates the interval in seconds for sampling the history statistics data. The valid range is 1 - 3600, default value is 1800 seconds.
Buckets	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600; the default value is 50.
Buckets Granted	The number of data that will be saved in the RMON.

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.

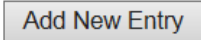
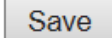
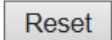
2.3.1.36 RMON Alarm

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



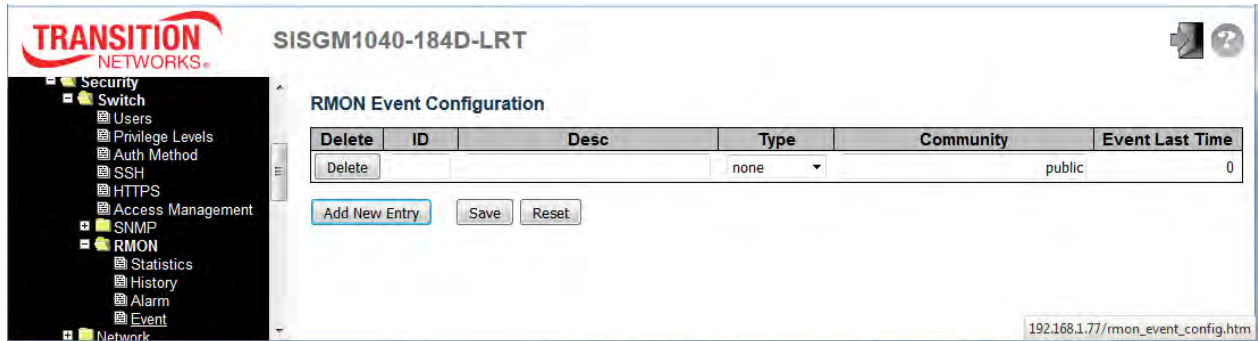
Object	Description
Delete	Check to delete the entry during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65.
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2 ³¹ -1.
Variable	Indicates the particular variable to be sampled, the possible variables are: InOctets : The total number of octets received on the interface, including framing characters. InUcastPkts : The number of uni-cast packets delivered to a higher-layer protocol. InNUcastPkts : The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. InDiscards : The number of inbound packets that are discarded even the packets are normal. InErrors : The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. InUnknownProtos : the number of the inbound packets that were discarded because of the unknown or un-support protocol. OutOctets : The number of octets transmitted out of the interface, including framing characters. OutUcastPkts : The number of uni-cast packets that request to transmit. OutNUcastPkts : The number of broad-cast and multi-cast packets that request to transmit. OutDiscards : The number of outbound packets that are discarded if the packets are normal. OutErrors : The number of outbound packets that could not be transmitted because of errors. OutQLen : The length of the output packet queue (in packets).
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

	<p>Absolute: Get the sample directly.</p> <p>Delta: Calculate the difference between samples (default).</p>
Value	The value of the statistic during the last sampling period.
Startup Alarm	<p>The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:</p> <p>Rising Trigger alarm when the first value is larger than the rising threshold.</p> <p>Falling Trigger alarm when the first value is less than the falling threshold.</p> <p>RisingOrFalling Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).</p>
Rising Threshold	Rising threshold value (-2147483648 - 2147483647).
Rising Index	Rising event index (1-65535).
Falling Threshold	Falling threshold value (-2147483648 - 2147483647).
Falling Index	Falling event index (1-65535).


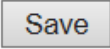
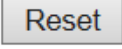
Buttons	
	Click to add a new community entry.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

2.3.1.37 RMON Event

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

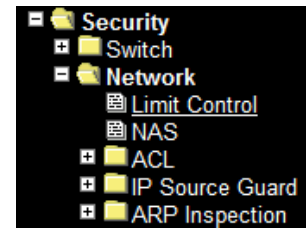


Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Desc	Indicates this event, the string length is from 0 to 127, default is a null string.
Type	Indicates the notification of the event, the possible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

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.

2.3.1.38 Network

2.3.1.39 Limit Control



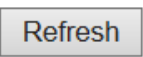
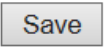
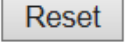
This page lets you configure the Port Security Limit Control system and port settings. Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four actions described below.

The Limit Control module utilizes a lower-layer (Port Security) module which manages MAC addresses learned on the port. The Limit Control configuration consists of two sections, a system- and a port-wide.

Object	Description
System Configuration	
Mode	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.
Aging Enabled	If checked, secured MAC addresses are subject to aging as discussed under Aging Period .

Aging Period	<p>If Aging Enabled 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	
Port	The port number to which the configuration below applies.
Mode	Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Note that other modules may still use the underlying port security features without enabling Limit Control on a given port.
Limit	<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 action 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>
Action	<p>If Limit is reached, the switch can take one of the following actions:</p> <p>None: Do not allow more than Limit MAC addresses on the port, but take no further action.</p> <p>Trap: If Limit + 1 MAC addresses are 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>Shutdown: If Limit + 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>

	<p>1) Boot the switch, 2) Disable and re-enable Limit Control on the port or the switch, 3) Click the Reopen button.</p> <p>Trap & Shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.</p>
State	<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>Disabled: Limit Control is either globally disabled or disabled on the port.</p> <p>Ready: The limit is not yet reached. This can be shown for all actions.</p> <p>Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap.</p> <p>Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.</p>
Re-open Button	<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 Shutdown in the Action 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 immediately. 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.

2.3.1.40 NAS

The **Configuration > Security > Network > NAS** page lets you 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 described 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-wide section and a port-wide section.

TRANSITION NETWORKS SISGM1040-184D-LRT

Open All / Close All

- System Information
- Front Panel
- Configuration
 - System
 - Green Ethernet
 - Ports
 - DHCP
 - Security
 - Switch
 - Network
 - Limit Control
 - NAS
 - ACL
 - IP Source Guard
 - ARP Inspection
 - AAA
 - Aggregation
 - Loop Protection
 - Spanning Tree
 - IPMC Profile
 - MVR
 - IPMC
 - LLDP
 - MAC Table
 - VLANs
 - Private VLANs
 - VCL
 - Voice VLAN
 - QoS
 - Mirroring
 - GVRP
 - sFlow
 - Redundant Ring&Chain
 - DDMI
 - Monitor
 - Diagnostics
 - Maintenance

Network Access Server Configuration

System Configuration

Mode	Disabled
Reauthentication Enabled	<input type="checkbox"/>
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	<input type="checkbox"/>
RADIUS-Assigned VLAN Enabled	<input type="checkbox"/>
Guest VLAN Enabled	<input type="checkbox"/>
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	<input type="checkbox"/>

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart
* <>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
1	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
2	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
3	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
4	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
5	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
6	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
7	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
8	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
9	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
10	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
11	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
12	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize

Save Reset

192.168.1.77/nas.htm

Object	Description
System Configuration	
Mode	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.
Reauthentication Enabled	<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 Aging Period below).</p>
Reauthentication Period	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.
EAPOL Timeout	Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.
Aging Period	<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"> • Single 802.1X • Multi 802.1X • MAC-Based Auth. <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 reauthentication 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, reauthentication 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>

Hold Time	<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"> • Single 802.1X • Multi 802.1X • MAC-Based Auth. <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>
RADIUS-Assigned QoS Enabled	<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 RADIUS-Assigned QoS Enabled 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 individual ports' ditto setting determines whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.</p>
RADIUS-Assigned VLAN Enabled	<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 RADIUS-Assigned VLAN Enabled 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 determines whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.</p>
Guest VLAN Enabled	<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</p>

	<p>switch follows a set of rules for entering and leaving the Guest VLAN as listed below. 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>
Guest VLAN ID	<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 globally enabled. Valid values are in the range [1; 4095].</p>
Max. Reauth. Count	<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. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].</p>
Allow Guest VLAN if EAPOL Seen	<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. The value can only be changed if the Guest VLAN option is globally enabled.</p>
Port Configuration	
Port	The port number for which the configuration below applies.
Admin State	<p>If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:</p> <p>Force Authorized: 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>Force Unauthorized: 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>Port-based 802.1X: 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</p>

LANs) frames. EAPOL frames encapsulate EAP PDUs ([RFC3748](#)). Frames sent between the switch and the RADIUS server are [RADIUS](#) 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 MD5-Challenge, PEAP, and TLS. 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.

Note: 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 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.

Single 802.1X: 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 Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X: 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 Port Security module.

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, 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 Port Security Limit Control functionality.

MAC-based Auth: 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 MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

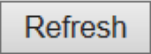
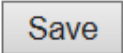
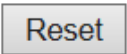
When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication,

	<p>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 Port Security Limit Control functionality.</p>
<p>RADIUS-Assigned QoS Enabled</p>	<p>When RADIUS-Assigned QoS is both globally 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 to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes (Port-based 802.1X or Single 802.1X).</p> <p><u>RADIUS attributes used in identifying a QoS Class:</u></p> <p>The User-Priority-Table attribute defined in RFC4675 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"> • 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].
<p>RADIUS-Assigned VLAN Enabled</p>	<p>When RADIUS-Assigned VLAN is both globally 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</p>

	<p>changed by the administrator in the meanwhile without affecting the RADIUS-assigned).</p> <p>This option is only available for single-client modes, either:</p> <ul style="list-style-type: none"> • Port-based 802.1X, or • Single 802.1X <p>For troubleshooting 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><u>RADIUS attributes used in identifying a VLAN ID:</u></p> <p>RFC2868 and RFC3580 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"> • The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet. • The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag): <ul style="list-style-type: none"> - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6). - Value of Tunnel-Type must be set to "VLAN" (ordinal 13). - Value of Tunnel-Private-Group-ID 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].
<p>Guest VLAN Enabled</p>	<p>When Guest VLAN is both globally 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"> • Port-based 802.1X • Single 802.1X • Multi 802.1X <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><u>Guest VLAN Operation:</u></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 Max. Reauth. Count and no EAPOL frames have been received in the</p>

	<p>meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen 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 Admin State 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> <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.</p>
<p>Port State</p>	<p>The current state of the port. It can undertake one of the following values:</p> <p>Globally Disabled: NAS is globally disabled.</p> <p>Link Down: NAS is globally enabled, but there is no link on the port.</p> <p>Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.</p> <p>Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.</p> <p>X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.</p>
<p>Restart</p>	<p>Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode.</p> <p>Clicking these buttons will not cause settings changed on the page to take effect.</p> <p>Reauthenticate: 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>Reinitialize: Forces a reinitialization of the clients on the port and thereby an</p>

	immediate reauthentication. The clients will transfer to the unauthorized state while the reauthentication is in progress.
--	----------------------------------------------------------------------------------------------------------------------------

Buttons	
	Click to refresh the page immediately. 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.

2.3.1.41 ACL

2.3.1.42 ACL Port

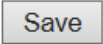
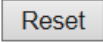
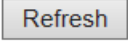
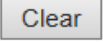
Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

The screenshot shows the 'ACL Ports Configuration' page in the Transition Networks web interface. The page title is 'SISGM1040-184D-LRT'. On the left is a navigation tree with categories like System Information, Configuration, Ports, Security, Network, and Monitor. The main area contains a table with columns: Port, Policy ID, Action, Rate Limiter ID, Port Redirect, Mirror, Logging, Shutdown, State, and Counter. The table lists 12 ports, each with a Policy ID of 0 and an Action of 'Permit'. The Rate Limiter ID is 'Disabled' for all. The Port Redirect column shows 'Disabled' for Port 1 and 'Port 2' for Port 2. The Mirror, Logging, and Shutdown columns are all 'Disabled'. The State column is 'Enabled' for all. The Counter column shows values ranging from 0 to 30289. At the bottom of the table are 'Save' and 'Reset' buttons. The URL in the bottom left corner is '192.168.1.77/acl_ports.htm'.

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	30289
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	3
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	6
4	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	77
5	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	41
6	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	3
7	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	21
8	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
10	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
11	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
12	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

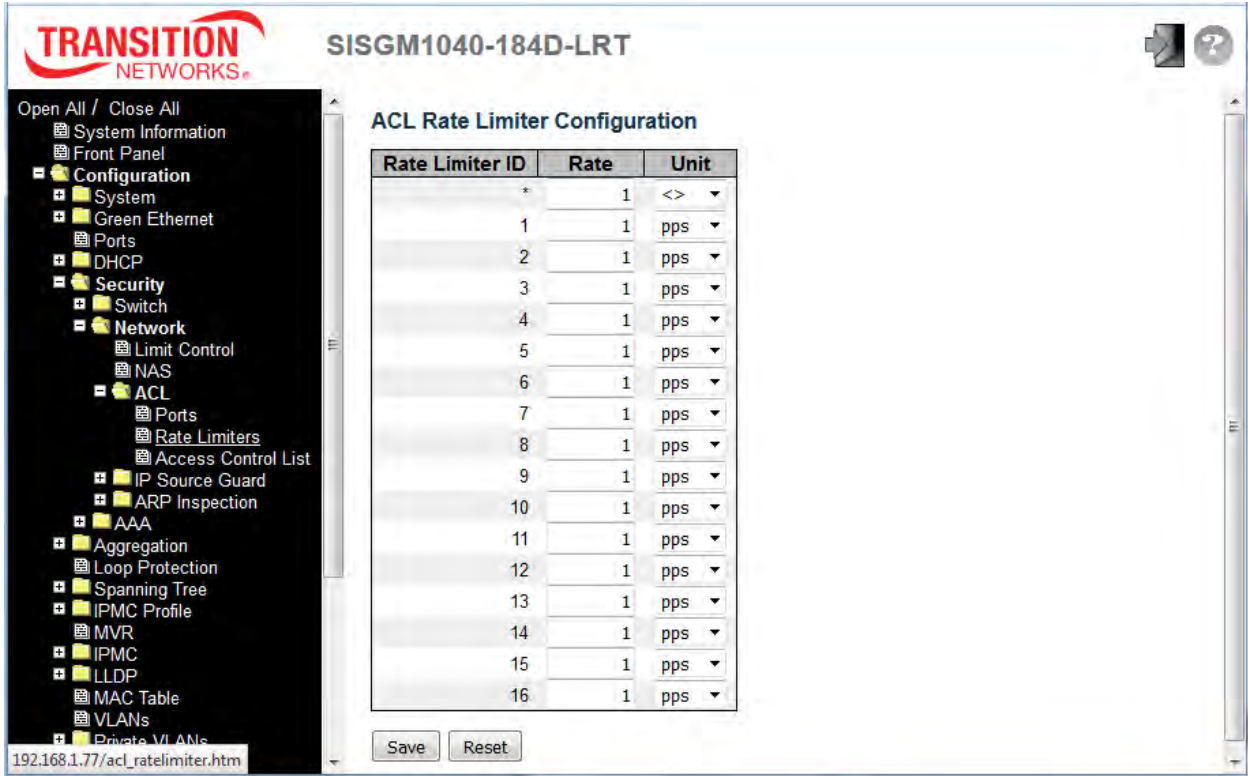
Object	Description
Port	The logical port for the settings contained in the same row.
Policy ID	Select the policy to apply to this port. The allowed values are 0 through 255. The default value is 0.
Action	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
Rate Limiter ID	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".

Port Redirect	Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled".
Mirror	Specify the mirror operation of this port. The allowed values are: Enabled : Frames received on the port are mirrored. Disabled : Frames received on the port are not mirrored. The default value is "Disabled".
Logging	Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC. The allowed values are: Enabled : Frames received on the port are stored in the System Log. Disabled : 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.
Shutdown	Specify the port shut down operation of this port. The allowed values are: Enabled : If a frame is received on the port, the port will be disabled. Disabled : 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).
State	Specify the port state of this port. The allowed values are: Enabled : To reopen ports by changing the volatile port configuration of the ACL user module. Disabled : To close ports by changing the volatile port configuration of the ACL user module. The default value is "Enabled".
Counter	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.
	Click to clear the counters.

2.3.1.43 ACL Rate Limiters

Configure the rate limiter for the ACL of the switch.



Object	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate	The rate range is 0–3276700 in pps, or 0, 100, 200, 300, . . . 1000000 in kbps.
Unit	Specify the rate unit of measure. The allowed values are: pps : packets per second. kbps : Kbits per second.

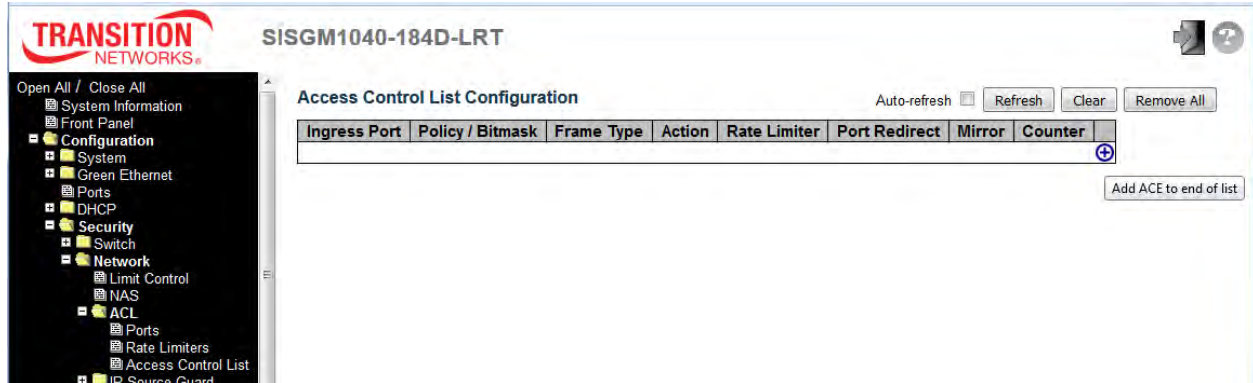
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

2.3.1.44 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 plus sign (+) to add a new ACE to the list. The reserved ACEs, used for internal protocols, cannot be edited or deleted; the order sequence cannot be changed, and the priority is highest.



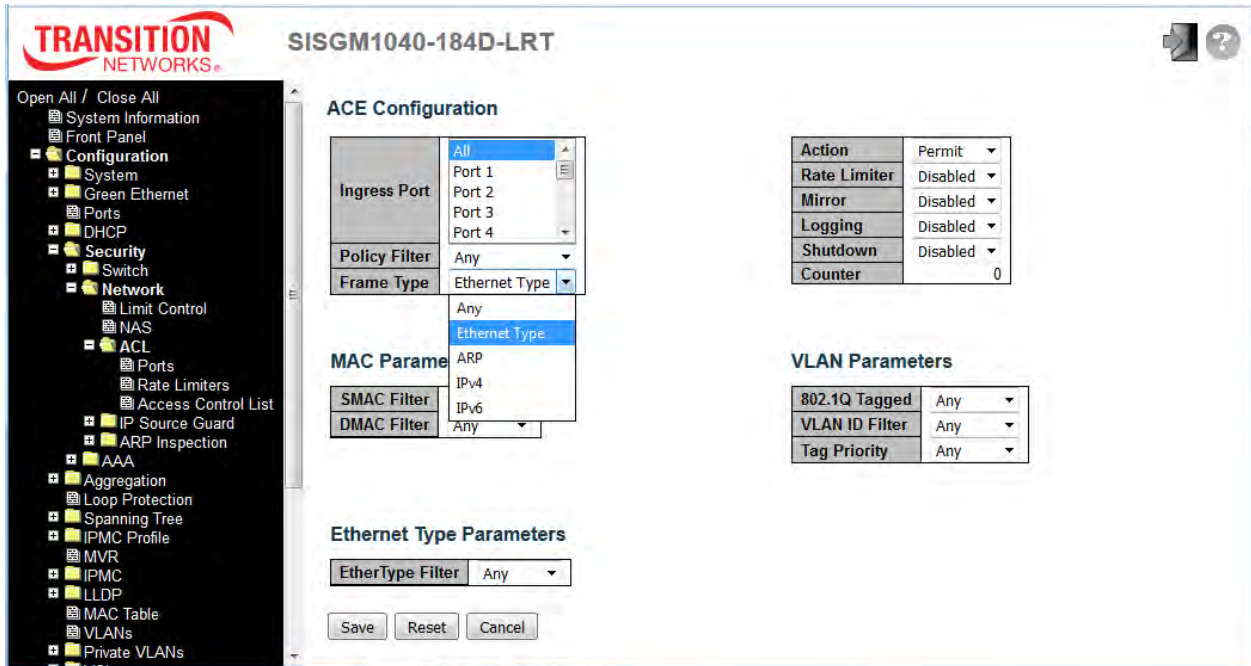
Object	Description
Ingress Port	Indicates the ingress port of the ACE. Possible values are: All : The ACE will match all ingress port. Port : The ACE will match a specific ingress port.
Policy / Bitmask	Indicates the policy number and bitmask of the ACE.
Frame Type	Indicates the frame type of the ACE. Possible values are: Any : The ACE will match any frame type. EType : The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ARP : The ACE will match ARP/RARP frames. IPv4 : The ACE will match all IPv4 frames. IPv4/ICMP : The ACE will match IPv4 frames with ICMP protocol. IPv4/UDP : The ACE will match IPv4 frames with UDP protocol. IPv4/TCP : The ACE will match IPv4 frames with TCP protocol. IPv4/Other : The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. IPv6 : The ACE will match all IPv6 standard frames.
Action	Indicates the forwarding action of the ACE. Permit : Frames matching the ACE may be forwarded and learned. Deny : Frames matching the ACE are dropped. Filter : Frames matching the ACE are filtered.

Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16 . When Disabled is displayed, the rate limiter operation is disabled.
Port Redirect	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

Mirror	Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are: Enabled : Frames received on the port are mirrored. Disabled : Frames received on the port are not mirrored. The default value is "Disabled".
Counter	The counter indicates the number of times the ACE was hit by a frame.
Modification Buttons	You can modify each ACE (Access Control Entry) in the table using these buttons:  : Inserts a new ACE before the current row.  : Edits the ACE row.  : Moves the ACE up the list.  : Moves the ACE down the list.  : Deletes the ACE.  : The lowest plus sign adds a new entry at the bottom of the ACE listings.

Buttons	
<input type="checkbox"/> Auto-refresh	Check this box to refresh the page automatically every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page; any changes made locally will be undone.
<input type="button" value="Clear"/>	Click to clear the counters.
<input type="button" value="Remove All"/>	Click to remove all ACEs.

The ACE Configuration page includes various fields, depending on the parameters chosen; for example:



Object	Description
Ingress Port	Select the ingress port for which this ACE applies. All : The ACE applies to all port. Port n : The ACE applies to this port number, where <i>n</i> is the number of the switch port.
Policy Filter	Specify the policy number filter for this ACE. Any : No policy filter is specified. (policy filter status is "don't-care".) Specific : If you want to filter a specific policy with this ACE, choose this value. Two field for entering a policy value and a policy bitmask display.
Policy Value	When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 to 255 .
Policy Bitmask	When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0xff . 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 & 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.
Frame Type	Select the frame type for this ACE. These frame types are mutually exclusive. Any : Any frame can match this ACE. Ethernet Type : 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

	<p>1536 decimal (equal to 0600 hexadecimal).</p> <p>ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type.</p> <p>IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.</p> <p>IPv6: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.</p>
Action	<p>Specify the action to take with a frame that hits this ACE.</p> <p>Permit: The frame that hits this ACE is granted permission for the ACE operation.</p> <p>Deny: The frame that hits this ACE is dropped.</p> <p>Filter: Frames matching the ACE are filtered.</p>
Rate Limiter	<p>Specify the rate limiter in number of base units. The allowed range is 1 to 16. Disabled indicates that the rate limiter operation is disabled.</p>
Port Redirect	<p>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. Disabled indicates that the port redirect operation is disabled and the specific port number of 'Port Redirect' can't be set when action is permitted.</p>
Mirror	<p>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:</p> <p>Enabled: Frames received on the port are mirrored.</p> <p>Disabled: Frames received on the port are not mirrored.</p> <p>The default value is "Disabled".</p>
Logging	<p>Specify the logging operation of the ACE. Notice that the logging message doesn't include the 4 bytes CRC information. The allowed values are:</p> <p>Enabled: Frames matching the ACE are stored in the System Log.</p> <p>Disabled: Frames matching the ACE are not logged.</p> <p>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.</p>
Shutdown	<p>Specify the port shut down operation of the ACE. The allowed values are:</p> <p>Enabled: If a frame matches the ACE, the ingress port will be disabled.</p> <p>Disabled: Port shut down is disabled for the ACE.</p> <p>Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).</p>
Counter	<p>The counter indicates the number of times the ACE was hit by a frame.</p>

MAC Parameters	
SMAC Filter	<p><i>(Only displayed when the frame type is Ethernet Type or ARP.)</i></p> <p>Specify the source MAC filter for this ACE.</p> <p>Any: No SMAC filter is specified. (SMAC filter status is "don't-care".)</p> <p>Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.</p>
SMAC Value	<p>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.</p>
DMAC Filter	<p>Specify the destination MAC filter for this ACE.</p> <p>Any: No DMAC filter is specified. (DMAC filter status is "don't-care".)</p> <p>MC: Frame must be multicast.</p> <p>BC: Frame must be broadcast.</p> <p>UC: Frame must be unicast.</p> <p>Specific: 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>
DMAC Value	<p>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.</p>
VLAN Parameters	
802.1Q Tagged	<p>Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are:</p> <p>Any: Any value is allowed ("don't-care").</p> <p>Enabled: Tagged frame only.</p> <p>Disabled: Untagged frame only.</p> <p>The default value is "Any".</p>
VLAN ID Filter	<p>Specify the VLAN ID filter for this ACE.</p> <p>Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)</p> <p>Specific: 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>
VLAN ID	<p>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.</p>
Tag Priority	<p>Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority.</p>

	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 Any means that no tag priority is specified (tag priority is "don't-care".)
ARP Parameters	
ARP/RARP	Specify the available ARP/RARP opcode (OP) flag for this ACE. Any : No ARP/RARP OP flag is specified. (OP is "don't-care".) ARP : Frame must have ARP opcode set to ARP. RARP : Frame must have RARP opcode set to RARP. Other : Frame has unknown ARP/RARP Opcode flag.
Request/Reply	Specify the available Request/Reply opcode (OP) flag for this ACE. Any : No Request/Reply OP flag is specified. (OP is "don't-care".) Request : Frame must have ARP Request or RARP Request OP flag set. Reply : Frame must have ARP Reply or RARP Reply OP flag.
Sender IP Filter	Specify the sender IP filter for this ACE. Any : No sender IP filter is specified. (Sender IP filter is "don't-care".) Host : Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears. Network : 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.
Sender IP Address	When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.
Sender IP Mask	When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.
Target IP Filter	Specify the target IP filter for this specific ACE. Any : No target IP filter is specified. (Target IP filter is "don't-care".) Host : Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears. Network : 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.
Target IP Address	When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.
Target IP Mask	When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.
ARP Sender MAC Match	Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. 0 : ARP frames where SHA is not equal to the SMAC address.

	<p>1: ARP frames where SHA is equal to the SMAC address.</p> <p>Any: Any value is allowed ("don't-care").</p>
RARP Target MAC Match	<p>Specify whether frames can hit the action according to their target hardware address field (THA) settings.</p> <p>0: RARP frames where THA is not equal to the target MAC address.</p> <p>1: RARP frames where THA is equal to the target MAC address.</p> <p>Any: Any value is allowed ("don't-care").</p>
IP/Ethernet Length	<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>0: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).</p> <p>1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).</p> <p>Any: Any value is allowed ("don't-care").</p>
IP	<p>Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.</p> <p>0: ARP/RARP frames where the HLD is not equal to Ethernet (1).</p> <p>1: ARP/RARP frames where the HLD is equal to Ethernet (1).</p> <p>Any: Any value is allowed ("don't-care").</p>
Ethernet	<p>Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.</p> <p>0: ARP/RARP frames where the PRO is not equal to IP (0x800).</p> <p>1: ARP/RARP frames where the PRO is equal to IP (0x800).</p> <p>Any: Any value is allowed ("don't-care").</p>
IP Parameters	
IP Protocol Filter	<p>Specify the IP protocol filter for this ACE.</p> <p>Any: No IP protocol filter is specified ("don't-care").</p> <p>Specific: 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>ICMP: 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>UDP: 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>TCP: 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>

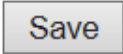
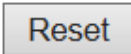
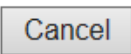
IP Protocol Value	When "Specific" is selected for the IP protocol value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IP protocol value.
IP TTL	Specify the Time-to-Live settings for this ACE. zero : IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry. non-zero : IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry. Any : Any value is allowed ("don't-care").
IP Fragment	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. No : IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry. Yes : IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry. Any : Any value is allowed ("don't-care").
IP Option	Specify the options flag setting for this ACE. No : IPv4 frames where the options flag is set must not be able to match this entry. Yes : IPv4 frames where the options flag is set must be able to match this entry. Any : Any value is allowed ("don't-care").
SIP Filter	Specify the source IP filter for this ACE. Any : No source IP filter is specified. (Source IP filter is "don't-care".) Host : Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears. Network : 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.
SIP Address	When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.
SIP Mask	When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
DIP Filter	Specify the destination IP filter for this ACE. Any : No destination IP filter is specified. (Destination IP filter is "don't-care".) Host : Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears. Network : 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.

DIP Address	When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.
DIP Mask	When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.
IPv6 Parameters	
Next Header Filter	<p>Specify the IPv6 next header filter for this ACE.</p> <p>Any: No IPv6 next header filter is specified ("don't-care").</p> <p>Specific: 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>ICMP: 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>UDP: Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.</p> <p>TCP: 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>
Next Header Value	When "Specific" is selected for the IPv6 next header value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IPv6 protocol value.
SIP Filter	<p>Specify the source IPv6 filter for this ACE.</p> <p>Any: No source IPv6 filter is specified. (Source IPv6 filter is "don't-care".)</p> <p>Specific: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear.</p>
SIP address	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.
SIP BitMask	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 & sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFFF (bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.
Hop Limit	<p>Specify the hop limit settings for this ACE.</p> <p>zero: IPv6 frames with a hop limit field greater than zero must not be able to match this entry.</p> <p>non-zero: IPv6 frames with a hop limit field greater than zero must be able to match this entry.</p>

	Any: Any value is allowed ("don't-care").
ICMP Parameters	
ICMP Type Filter	Specify the ICMP filter for this ACE. Any: No ICMP filter is specified (ICMP filter status is "don't-care"). Specific: 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.
ICMP Type Value	When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP value.
ICMP Code Filter	Specify the ICMP code filter for this ACE. Any: No ICMP code filter is specified (ICMP code filter status is "don't-care"). Specific: 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.
ICMP Code Value	When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value.
TCP/UDP Parameters	
TCP/UDP Source Filter	Specify the TCP/UDP source filter for this ACE. Any: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care"). Specific: 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. Range: 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.
TCP/UDP Source No.	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.
TCP/UDP Source Range	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.
TCP/UDP Destination Filter	Specify the TCP/UDP destination filter for this ACE. Any: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care"). Specific: If you want to filter a specific TCP/UDP destination filter with this ACE, you

	<p>can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.</p> <p>Range: 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>
TCP/UDP Destination Number	<p>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.</p>
TCP/UDP Destination Range	<p>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.</p>
TCP FIN	<p>Specify the TCP "No more data from sender" (FIN) value for this ACE.</p> <p>0: TCP frames where the FIN field is set must not be able to match this entry.</p> <p>1: TCP frames where the FIN field is set must be able to match this entry.</p> <p>Any: Any value is allowed ("don't-care").</p>
TCP SYN	<p>Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.</p> <p>0: TCP frames where the SYN field is set must not be able to match this entry.</p> <p>1: TCP frames where the SYN field is set must be able to match this entry.</p> <p>Any: Any value is allowed ("don't-care").</p>
TCP RST	<p>Specify the TCP "Reset the connection" (RST) value for this ACE.</p> <p>0: TCP frames where the RST field is set must not be able to match this entry.</p> <p>1: TCP frames where the RST field is set must be able to match this entry.</p> <p>Any: Any value is allowed ("don't-care").</p>
TCP PSH	<p>Specify the TCP "Push Function" (PSH) value for this ACE.</p> <p>0: TCP frames where the PSH field is set must not be able to match this entry.</p> <p>1: TCP frames where the PSH field is set must be able to match this entry.</p> <p>Any: Any value is allowed ("don't-care").</p>
TCP ACK	<p>Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.</p> <p>0: TCP frames where the ACK field is set must not be able to match this entry.</p> <p>1: TCP frames where the ACK field is set must be able to match this entry.</p> <p>Any: Any value is allowed ("don't-care").</p>
TCP URG	<p>Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.</p> <p>0: TCP frames where the URG field is set must not be able to match this entry.</p> <p>1: TCP frames where the URG field is set must be able to match this entry.</p> <p>Any: Any value is allowed ("don't-care").</p>

Ethernet Type Parameters	
EtherType Filter	<p>Specify the Ethernet type filter for this ACE.</p> <p>Any: No EtherType filter is specified (EtherType filter status is "don't-care").</p> <p>Specific: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering an EtherType value appears.</p>
Ethernet Type Value	<p>When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is 0x600 to 0xFFFF but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.</p>

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

2.3.1.45 IP Source Guard

IP Source Guard is a security feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

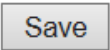
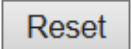
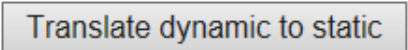
2.3.1.46 IP Source Guard Configuration

This page provides IP Source Guard related configuration.

The screenshot shows the web interface for configuring IP Source Guard. The left sidebar contains a navigation tree with 'IP Source Guard' selected. The main content area has a title 'IP Source Guard Configuration' and a 'Mode' dropdown set to 'Disabled'. A 'Translate dynamic to static' button is present. Below is a table for 'Port Mode Configuration' with 12 rows, each representing a port. All ports are currently set to 'Disabled' mode and 'Unlimited' max dynamic clients. 'Save' and 'Reset' buttons are at the bottom.

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
9	Disabled	Unlimited
10	Disabled	Unlimited
11	Disabled	Unlimited
12	Disabled	Unlimited

Object	Description
Mode of IP Source Guard Configuration	Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.
Port Mode Configuration	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.
Max Dynamic Clients	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.

2.3.1.47 IP Source Guard Static Table

This page provides IP Source Guard static table configuration.



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.
IP Address	Allowed Source IP address.
MAC address	Allowed Source MAC address.

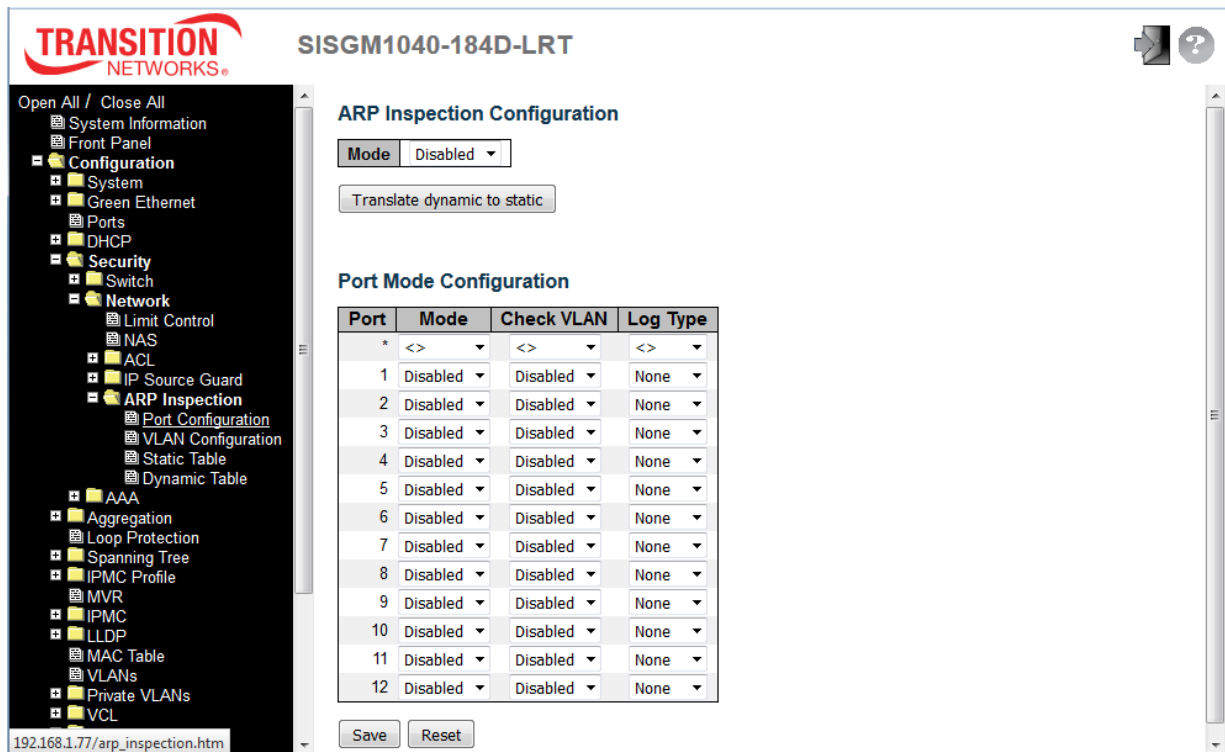
Buttons	
	Click to add a new entry to the Static IP Source Guard table.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

2.3.1.48 ARP Inspection

ARP Inspection is a security feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

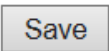
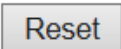
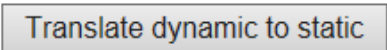
2.3.1.49 Port Configuration

This page provides ARP Inspection related configuration.



Object	Description
Mode of ARP Inspection Configuration	Enable the Global ARP Inspection or disable the Global ARP Inspection.
Port Mode Configuration	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. Possible modes are: Enabled: Enable ARP Inspection operation. Disabled: Disable ARP Inspection operation. 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

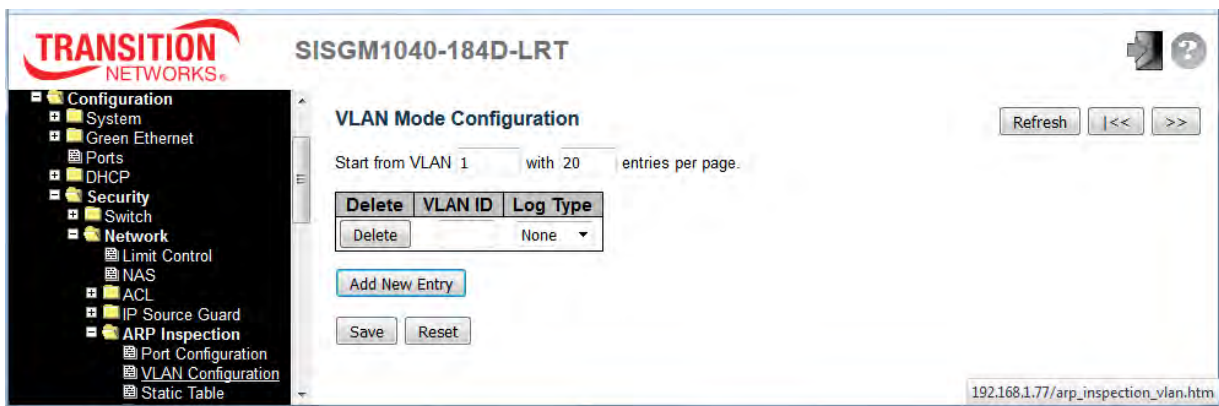
	<p>"Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting.</p> <p>Possible setting of "Check VLAN" are:</p> <p>Enabled: Enable check VLAN operation.</p> <p>Disabled: 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>None: Log nothing.</p> <p>Deny: Log denied entries.</p> <p>Permit: Log permitted entries.</p> <p>ALL: 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.

2.3.1.50 VLAN Mode 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 lets you 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 >> button will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached a warning message is shown in the displayed table. Use the **Reset** button to start over.



Specify ARP Inspection to be enabled on which VLANs. First, you must enable the port setting on the 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 the VLAN Mode Configuration web page. The Log Type also can be configured on a per VLAN setting.

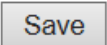
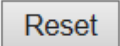

Possible Log Types are:

None: Log nothing.

Deny: Log denied entries.

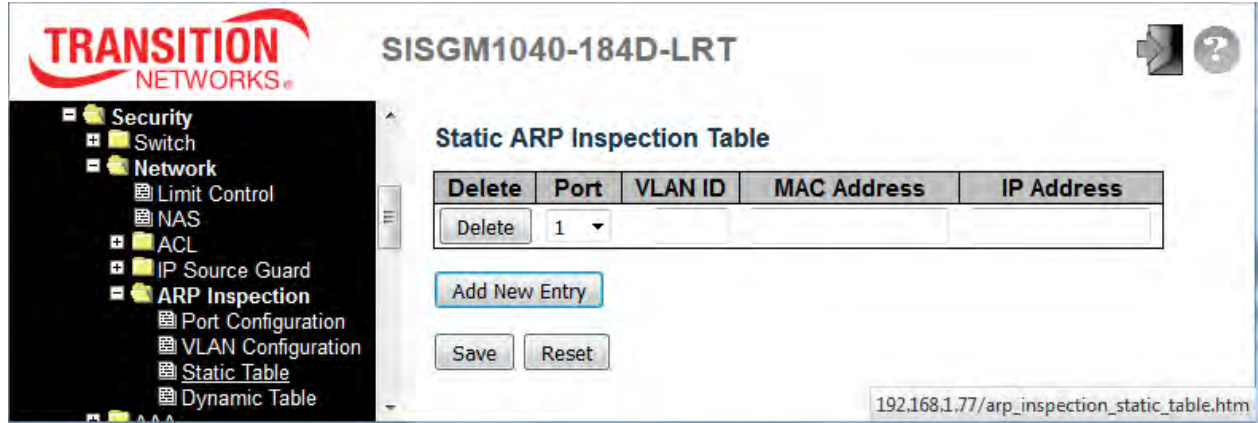
Permit: Log permitted entries.

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.

2.3.1.51 Static ARP Inspection Table


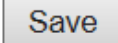
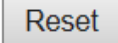
Click the **Add New Entry** button to add a new entry to the Static ARP Inspection Table for configuration.



The Static ARP Inspection Table parameters are described below.

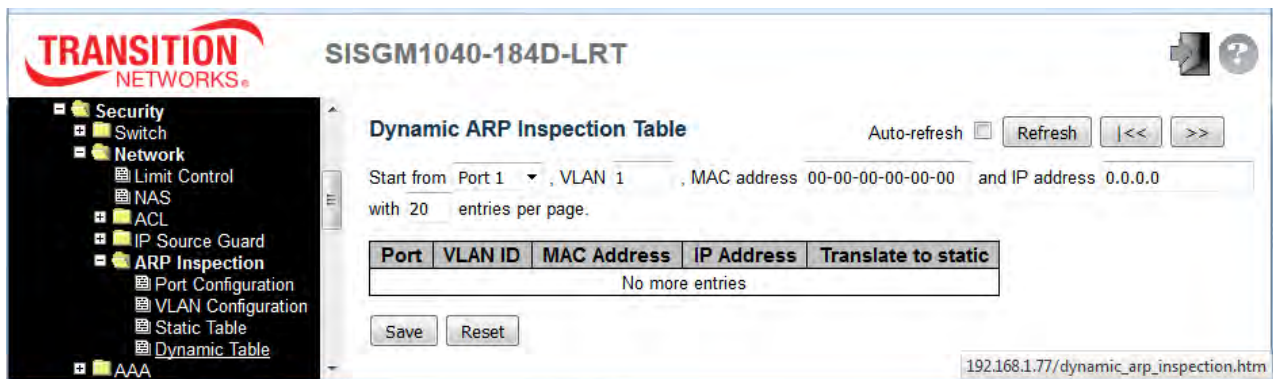
Object	Description
Delete	Check to delete the entry during the next save.
Port	The logical port for the settings.
VLAN ID	The VLAN ID (VID) for the settings.
MAC Address	Allowed Source MAC address in ARP request packets.
IP Address	Allowed Source IP address in ARP request packets.

The Static ARP Inspection Table buttons are described below.

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




2.3.1.52 Dynamic ARP Inspection Table

Each page shows up to 99 entries from the Dynamic ARP Inspection table (default 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 let you select the starting point in the Dynamic ARP Inspection Table. Click the |<< button to update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. 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 >> button 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" displays in the table. Use the **Reset** button to start over.



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

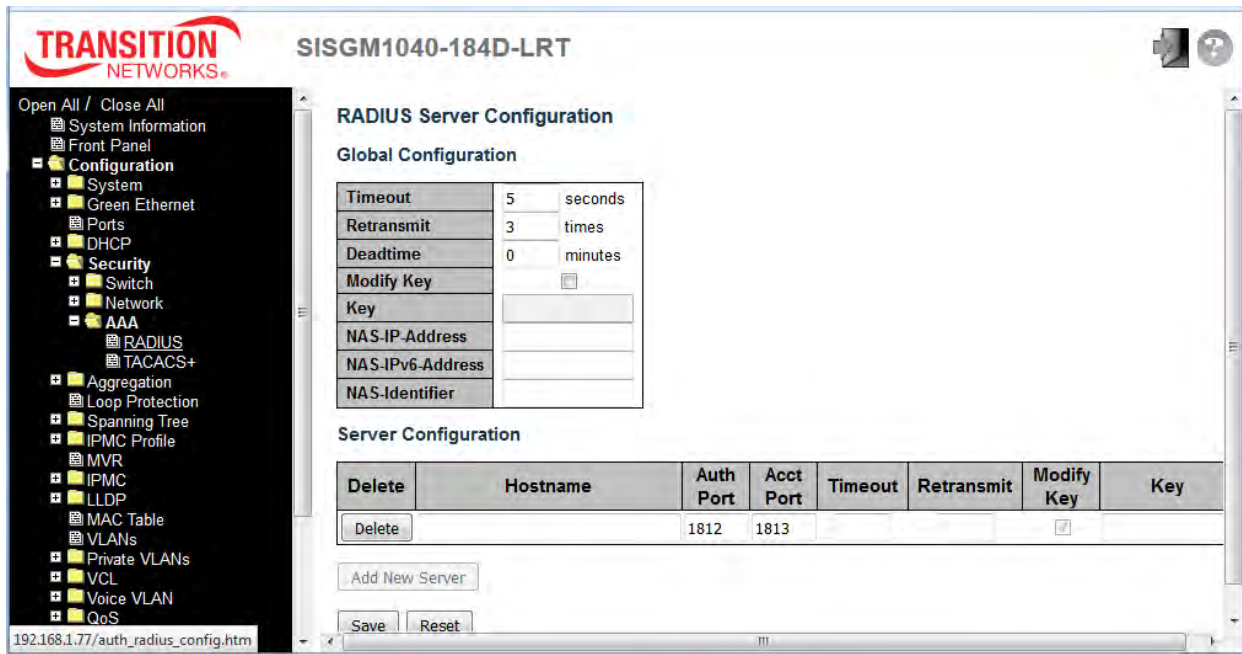
Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically every 3 seconds.
<input type="button" value="Refresh"/>	Refreshes the displayed table starting from the input fields.
<input type="button" value="Save"/>	Click to save changes.

	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.

2.3.1.53 AAA

2.3.1.54 RADIUS

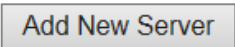

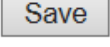
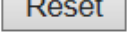
This page lets you configure up to five RADIUS servers.



Object	Description
Global Configuration	
Timeout	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.
Retransmit	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.
Deadtime	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.
Key	The secret key - up to 63 characters long - shared between the RADIUS server and the

	switch.
--	---------

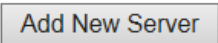

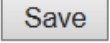
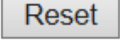
NAS-IP-Address (Attribute 4)	The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.
NAS-IPv6-Address (Attribute 95)	The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.
NAS-Identifier (Attribute 32)	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.
Server Configuration	
Delete	To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.
Hostname	The IP address or hostname of the RADIUS server.
Auth Port	The UDP port to use on the RADIUS server for authentication.
Acct Port	The UDP port to use on the RADIUS server for accounting.
Timeout	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
Retransmit	This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.
Key	This optional setting overrides the global key. Leaving it blank will use the global key.

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

2.3.1.55 TACACS+

This page lets you configure up to five TACACS+ servers.

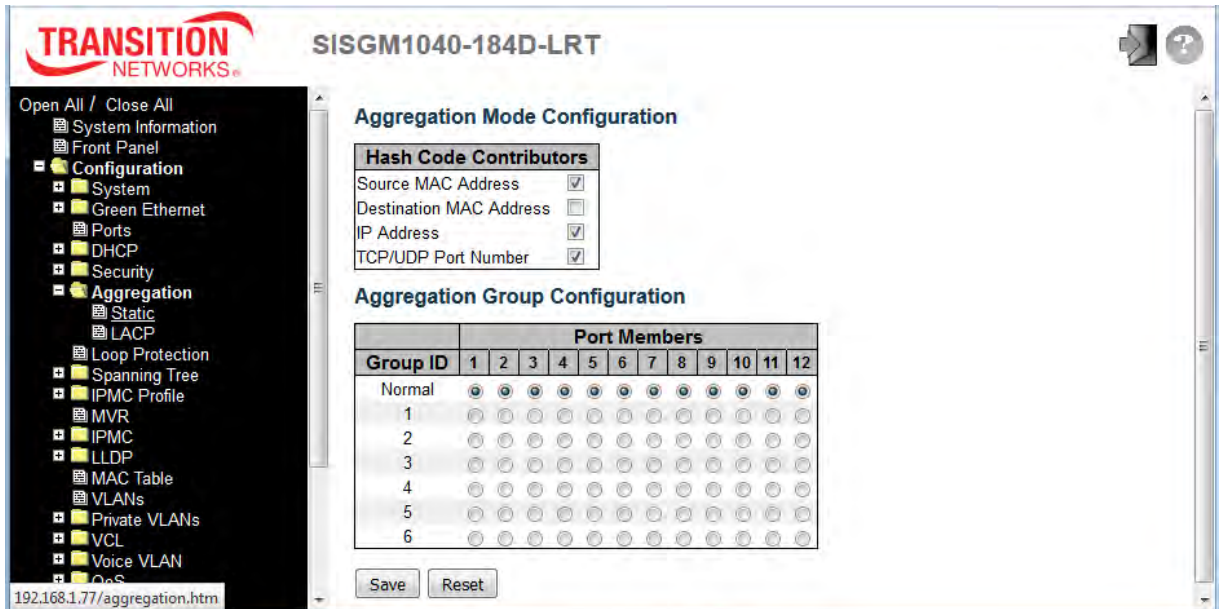
Object	Description
Global Configuration	
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.
Deadtime	Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will 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.
Key	The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.
Server Configuration	
Delete	Check this box to delete a TACACS+ server entry during the next Save.
Hostname	The IP address or hostname of the TACACS+ server.
Port	The TCP port to use on the TACACS+ server for authentication.
Timeout	This optional setting overrides the global timeout value. Leaving it blank uses the global timeout value.
Key	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.

2.3.1.56 Aggregation

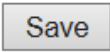
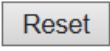
2.3.1.57 Static Aggregation

This page is used to configure the Aggregation hash mode and the aggregation group.



Object	Description
Hash Code Contributors	
Source MAC Address	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.
Destination MAC Address	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.
IP Address	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.
TCP/UDP Port Number	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.

Aggregation Group Configuration	
Group ID	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.
Port Members	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.

Note: Static aggregation and LACP cannot both be enabled on the same ports at the same time.

2.3.1.58 LACP Aggregation

This page lets you view and configure the current LACP port configuration parameters.

Note: Static aggregation and LACP cannot both be enabled on the same ports at the same time.

TRANSITION NETWORKS SISGM1040-184D-LRT

Open All / Close All

- System Information
- Front Panel
- Configuration
 - System
 - Green Ethernet
 - Ports
 - DHCP
 - Security
 - Aggregation
 - Static
 - LACP
 - Loop Protection
 - Spanning Tree
 - IPMC Profile
 - MVR
 - IPMC
 - LLDP
 - MAC Table
 - VLANs
 - Private VLANs
 - VCL
 - Voice VLAN
 - QoS
 - Mirroring
 - CVRR

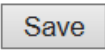
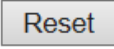
192.168.1.77/lacp_port_config.htm

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
9	<input type="checkbox"/>	Auto	Active	Fast	32768
10	<input type="checkbox"/>	Auto	Active	Fast	32768
11	<input type="checkbox"/>	Auto	Active	Fast	32768
12	<input type="checkbox"/>	Auto	Active	Fast	32768

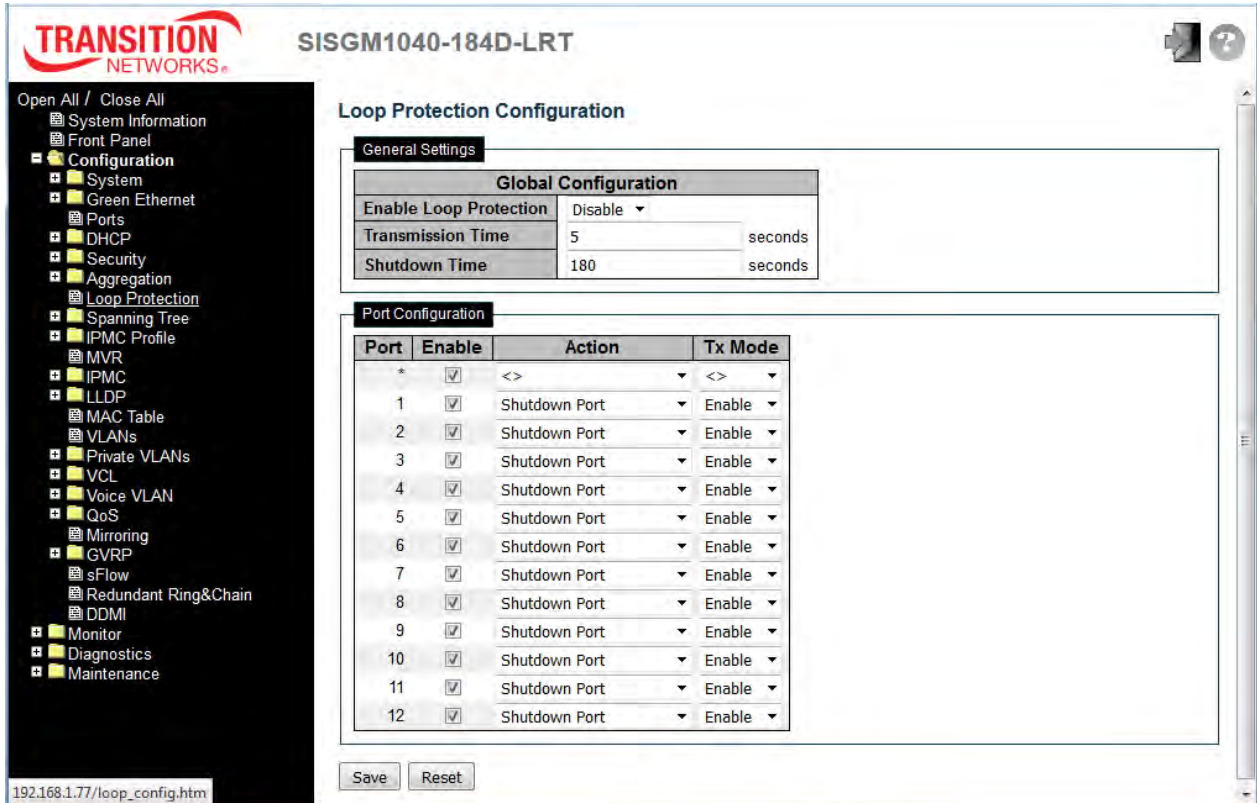
Save Reset

Object	Description
Port	The switch port number.
LACP Enabled	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.
Key	The Key value incurred by the port, range 1-65535. The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific 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.
Role	The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).
Timeout	The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.
Prio	The Prio 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.

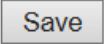
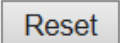
2.3.1.59 Loop Protection

This page lets you view or configure the current Loop Protection Configuration settings.

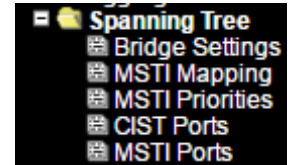


Object	Description
General Settings	
Enable Loop Protection	Controls whether loop protections is enabled (as a whole).
Transmission Time	The interval between each loop protection PDU sent on each port; valid values are 1 to 10 seconds.
Shutdown Time	The period (in seconds) for which a port will be kept 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).
Port Configuration	
Port	The switch port number of the port.
Enable	Controls whether loop protection is enabled on this switch port.
Action	Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port , Shutdown Port and Log or Log Only .

Tx Mode	Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.
----------------	-----------------------------------------------------------------------------------------------------------------------------------

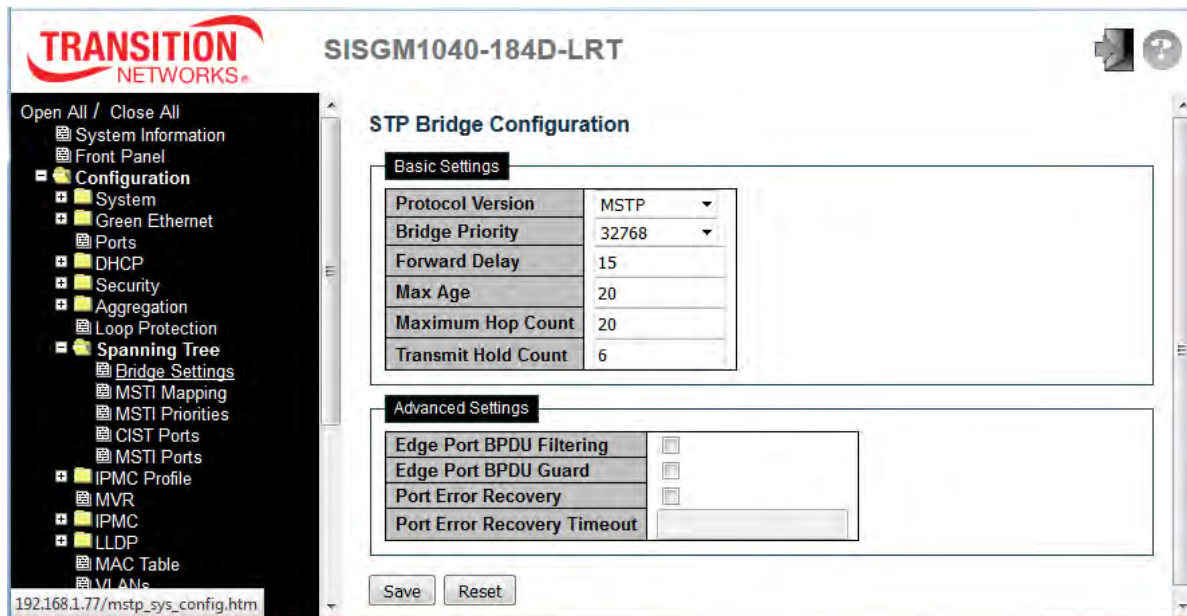
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

2.3.1.60 Spanning Tree



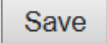
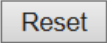
2.3.1.61 Bridge Settings

This page lets you configure the STP system settings that are used by all STP Bridge instances in the switch.



Object	Description
Basic Settings	
Protocol Version	The MSTP / RSTP / STP protocol version setting. Valid values are STP , RSTP and MSTP .
Bridge Priority	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 MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge
Forward Delay	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.
Max Age	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
Maximum Hop Count	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.
Transmit Hold Count	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.
Advanced Settings	
Edge Port BPDU Filtering	Control whether a port <i>explicitly</i> configured as Edge will transmit and receive BPDUs.
Edge Port BPDU Guard	Control whether a port <i>explicitly</i> configured as Edge 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.
Port Error Recovery	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.
Port Error Recovery Timeout	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).

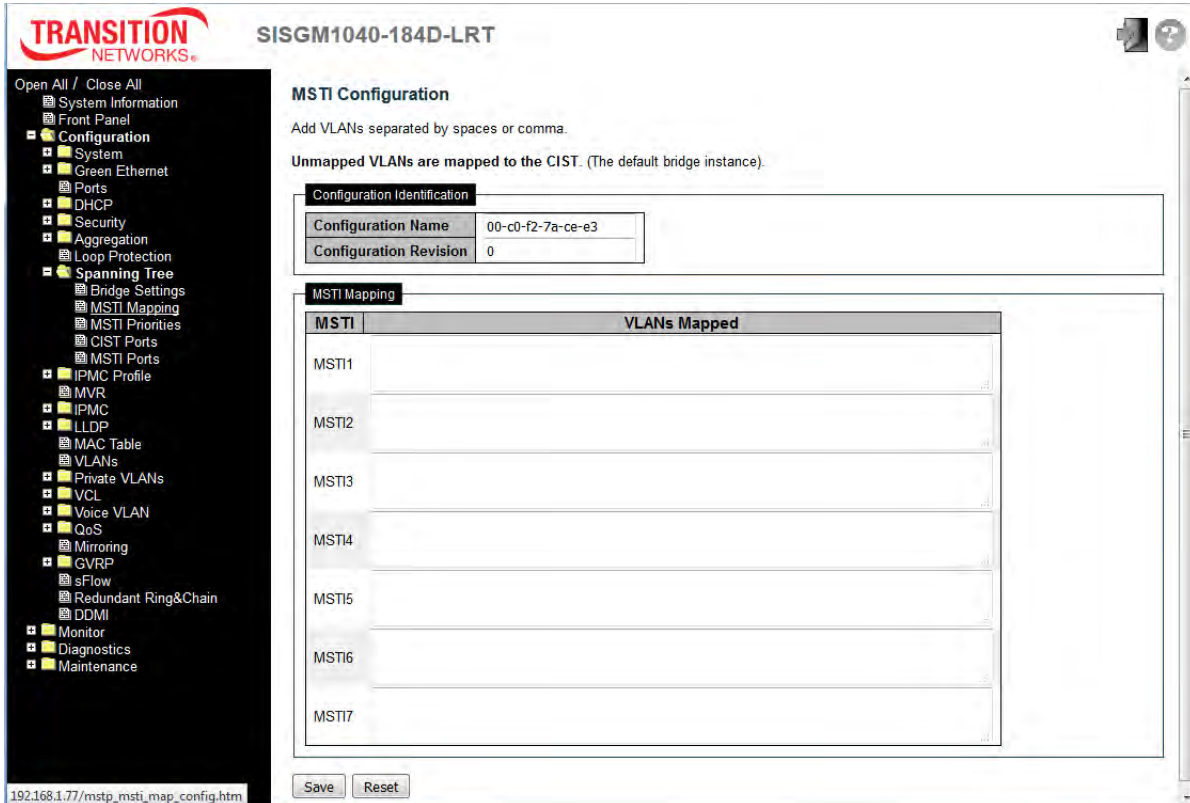
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

Messages

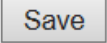
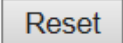
Message: *STP Error STP port configuration error. (notes: Before you enable STP ports, please disable all of Ring groups first.)*

2.3.1.62 MSTI Mapping

This page lets you view and configure current STP MSTI bridge instance priority settings.

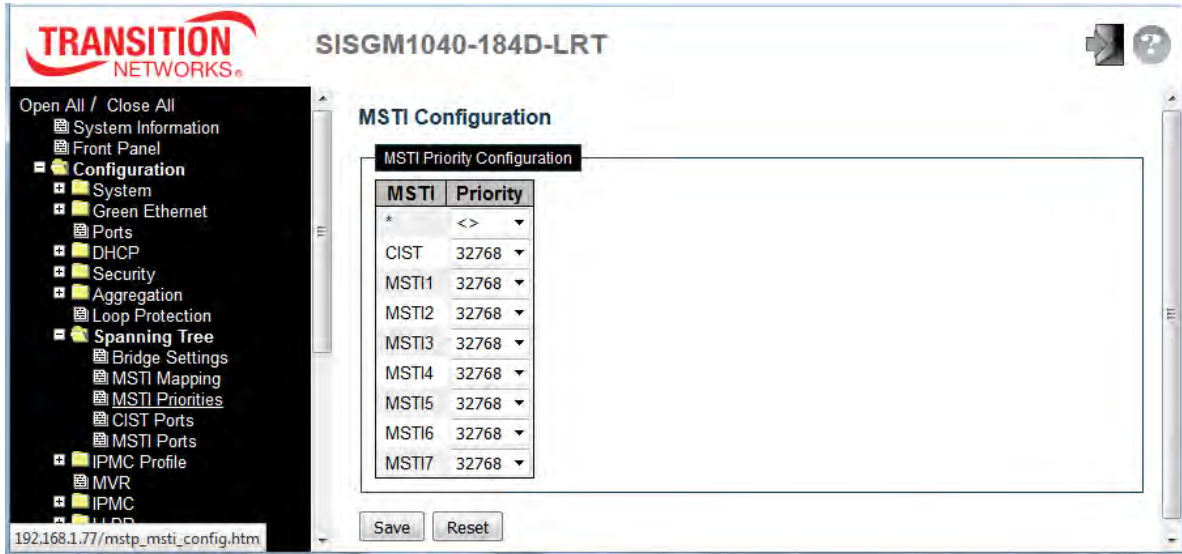


Object	Description
Configuration Identification	
Configuration Name	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name can be up to 32 characters.
Configuration Revision	The revision of the MSTI configuration named above. This must be 0 - 65535.
MSTI Mapping	
MSTI	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
VLANs Mapped	The list of VLANs mapped to the MSTI. The VLANs can be given as a single VLAN (1 - 4094), or a VLAN range, 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 must be left empty (i.e., not having any VLANs mapped to it). For example: 2, 5, 20-40 .

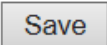
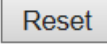
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

2.3.1.63 MSTI Priorities

This page lets you view and configure current STP MSTI bridge instance priority settings.

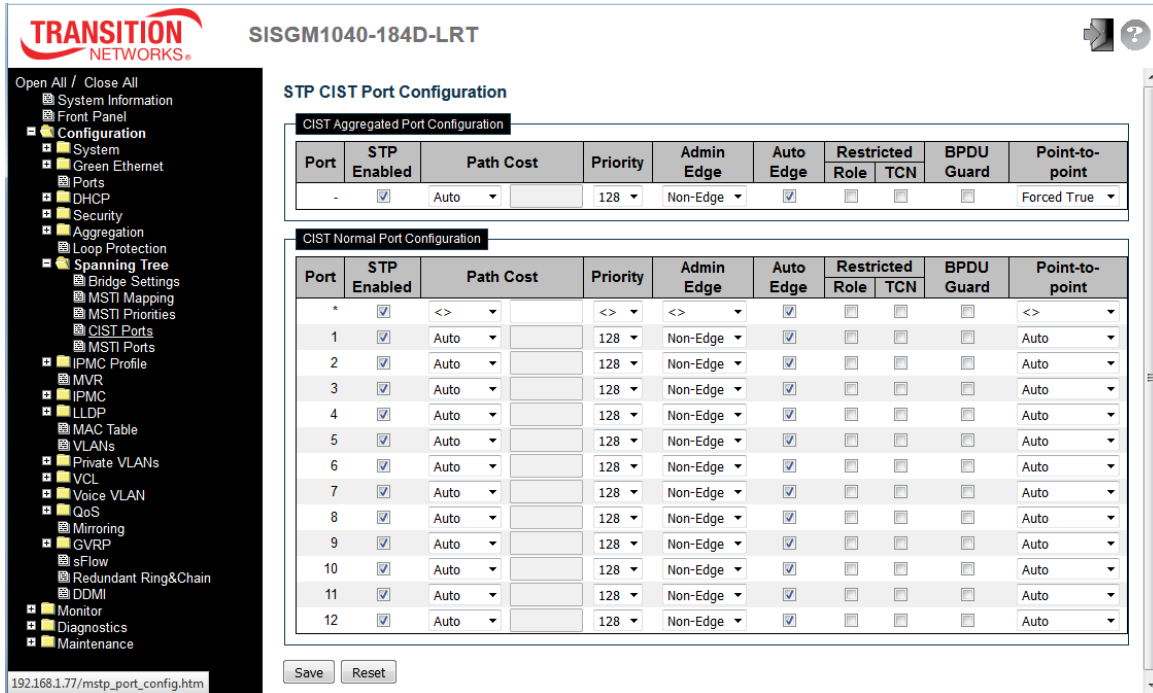


Object	Description
MSTI	The bridge instance. The CIST is the <i>default</i> instance, which is always active.
Priority	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms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

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

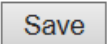
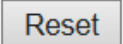
2.3.1.64 CIST Ports

This page lets you view and configure the current STP CIST port configuration settings. This page contains settings for physical ports and aggregated ports.



Object	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific 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 favor of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
operEdge (state flag)	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.
AdminEdge	Controls whether the <i>operEdge</i> flag should start as set or cleared. (The initial <i>operEdge</i> state when a port is initialized).
AutoEdge	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.
Restricted Role	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 Root Guard .
Restricted TCN	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.
BPDU Guard	If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not effect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.
Point-to-Point	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.

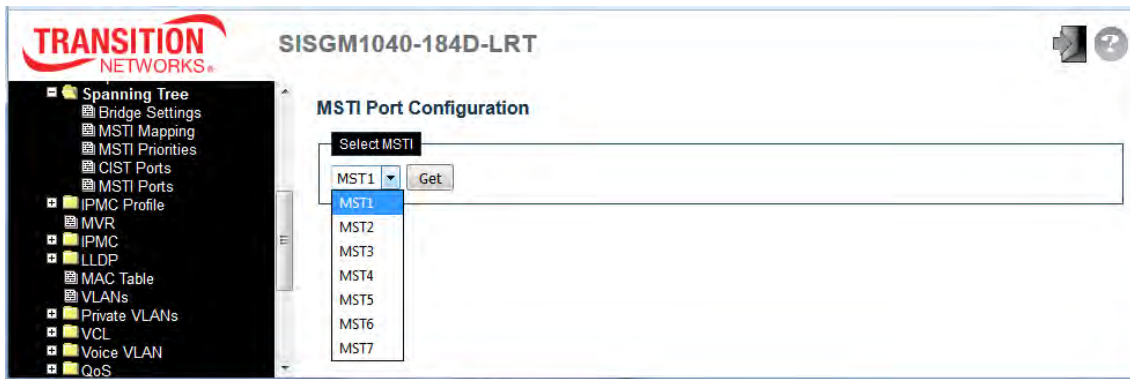
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

2.3.1.65 MSTI Ports

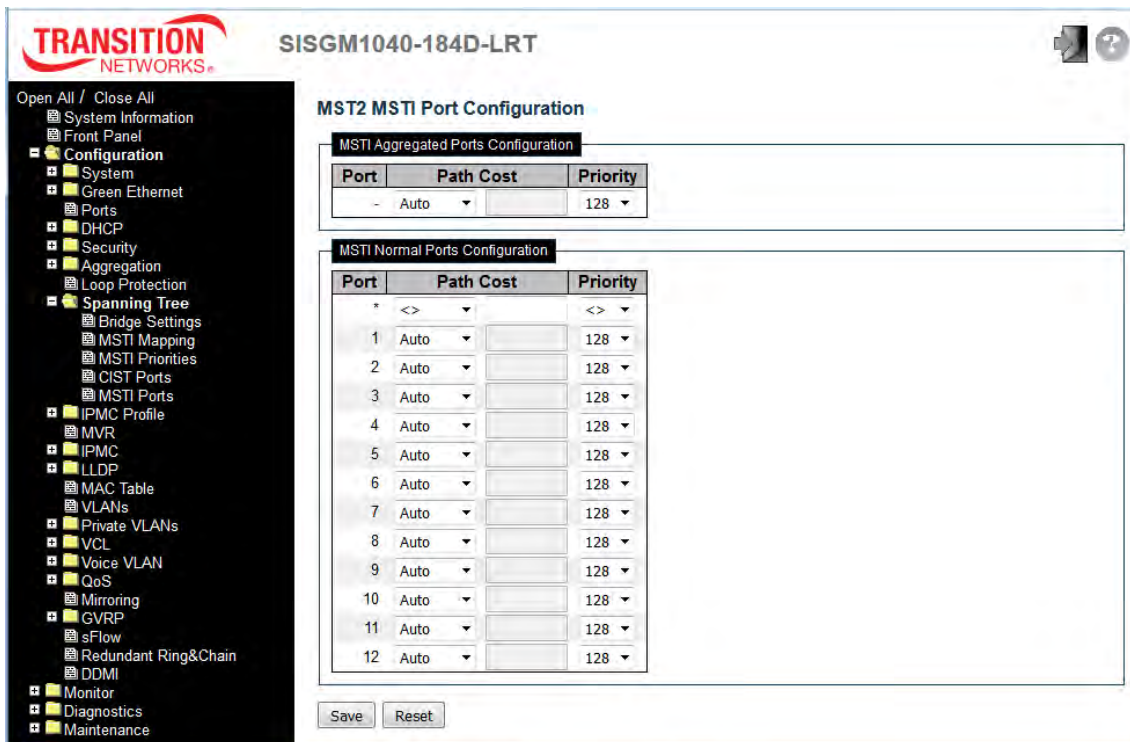
This page lets you view and modify the current STP MSTI port configurations.

A 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.



At the dropdown select an MSTI port. Click to get the selected MSTI settings; the page displays:



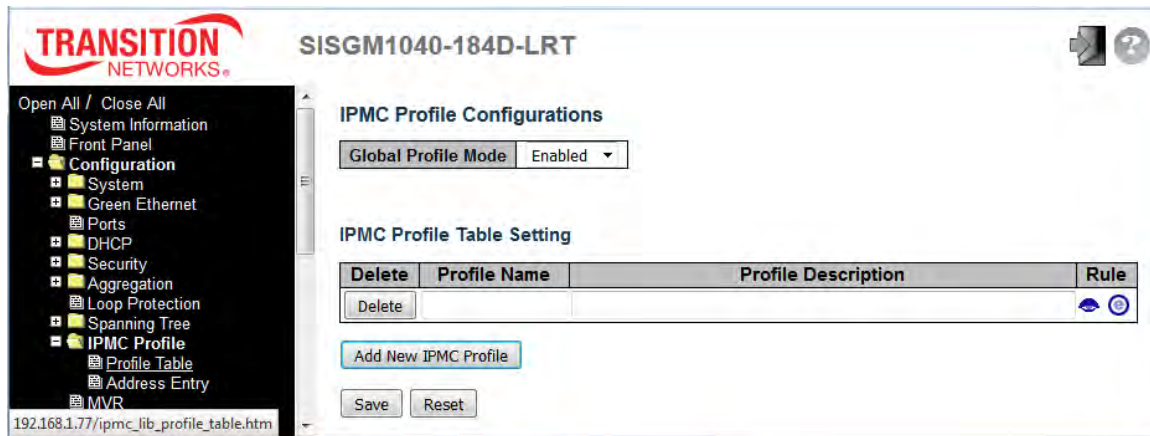
Object	Description
Port	The switch port number of the corresponding STP CIST (and MSTI) port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined 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 favor of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).



Buttons	
	Click to retrieve settings for a specific MSTI.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.


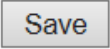
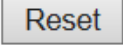
2.3.1.66 IPMC Profile

2.3.1.67 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
Global Profile Mode	Enable/Disable the Global IPMC Profile. The Switch starts to do filtering based on profile settings only when the global profile mode is enabled.
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
Profile Name	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.
Profile Description	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.
Rule	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:  : Navigate Profile Rules; list the rules associated with the designated profile.  : Edit Profile Rule; adjust the rules associated with the designated profile.

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.

The IPMC Profile Rule Settings for [Rule-1]:



TRANSITION NETWORKS SISGM1040-184D-LRT


IPMC Profile [Rule-1] Rule Settings (In Precedence Order)


Profile Name & Index	Entry Name	Address Range	Action	Log	
Rule-1	1	-	Deny	Disable	 


  

Navigation Icons:

 : Insert a new Rule before this Rule.

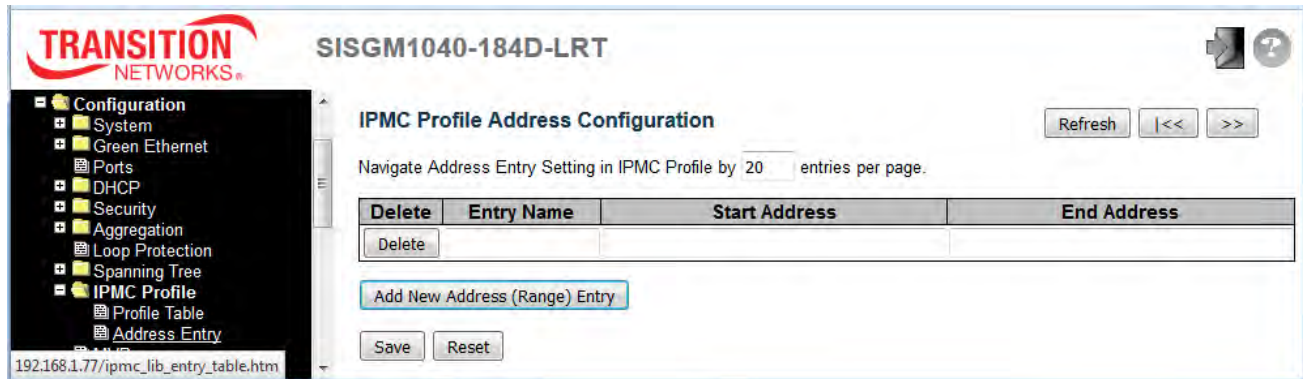
 : Delete this Rule.

 : Move this Rule up.

 : Move this Rule down.

2.3.1.68 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. You can create up to 128 address entries in the system.



Object	Description
Delete	Check to delete the entry during the next save.
Entry Name	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.
Start Address	The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.
End Address	The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

Buttons	
	Click to add a new address range. Specify the name and addresses.
	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.

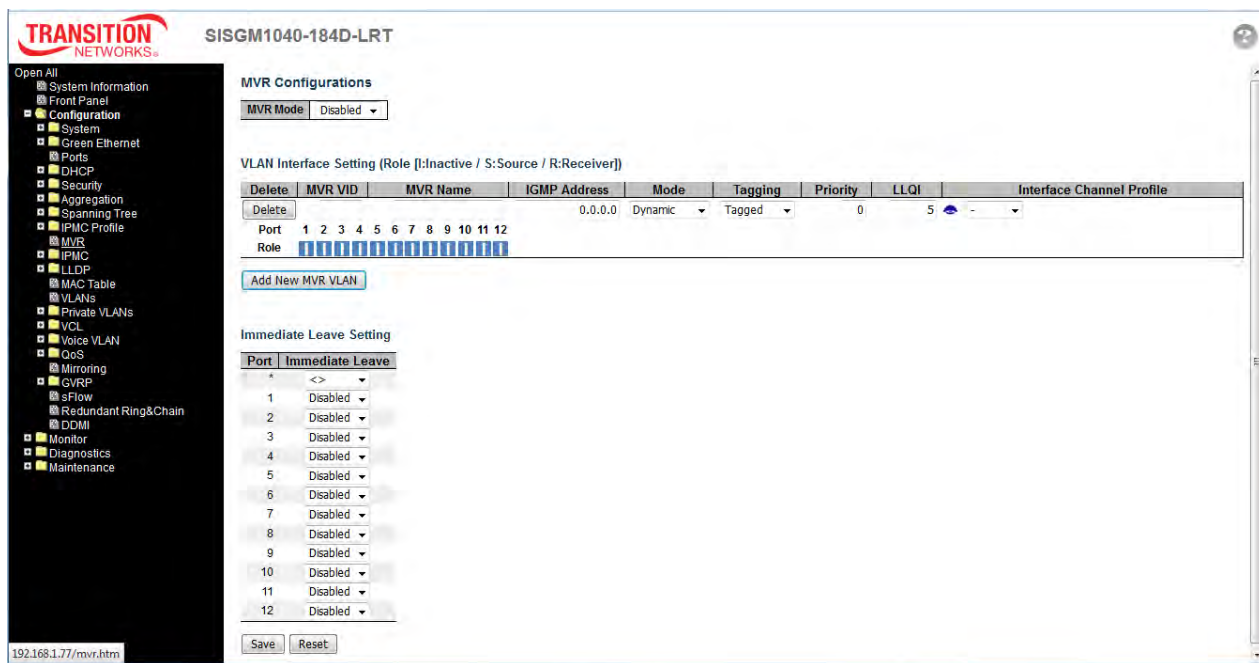
2.3.1.69 MVR

This page provides MVR related configuration. Most of the settings are global, whereas the Immediate Leave and MVR Port-Role configuration is related to the current selecting stack unit, as reflected by the page header.


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 four MVR VLANs with corresponding channel profile for each Multicast VLAN. The channel profile is defined by the IPMC Profile which provides the filtering conditions.



Object	Description
MVR Mode	Enable/Disable the Global MVR. The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.
Delete	Check to delete the entry. The designated entry will be deleted during the next save.

MVR VID	Specify the Multicast VLAN ID. Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.
MVR Name	MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. 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.
IGMP Address	Define the IPv4 address as source address used in IP header for IGMP control frames. The default IGMP address is not set (0.0.0.0). When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.
Mode	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.
Tagging	Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.
Priority	Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.
LLQI	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 second. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.
Interface Channel Profile	When the MVR VLAN is created, select the IPMC Profile 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.
Profile Management Button	You can inspect the rules of the designated profile by using the following button:  : Click to list the rules associated with the designated profile.
Port	The logical port for the settings.
Port Role	Configure an MVR port of the designated MVR VLAN as one of the following roles. Inactive: The designated port does not participate MVR operations. Source: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.

	<p>Receiver: 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>Caution: 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 (I).</p>
Immediate Leave	Enable the fast leave on the port.

Buttons	
<input type="button" value="Add New MVR VLAN"/>	Click to add new MVR VLAN. Specify the VID and configure the new entry. Click "Save".
<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.

2.3.1.70 IPMC

IPMC (IP MultiCast) supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6. An IPMC Profile is used to deploy the access control on IP multicast streams.

2.3.1.71 IGMP Snooping

IGMP (Internet Group Management Protocol) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

2.3.1.72 Basic Configuration

This page provides IGMP Snooping related configuration.

The screenshot displays the 'IGMP Snooping Configuration' page in the Transition Networks web interface. The left sidebar shows a navigation tree with 'Configuration' expanded to 'IPMC' and 'IGMP Snooping'. The main content area is divided into two sections:

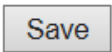
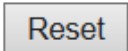
- Global Configuration:**
 - Snooping Enabled:
 - Unregistered IPMCv4 Flooding Enabled:
 - IGMP SSM Range: 232.0.0.0 / 8
 - Leave Proxy Enabled:
 - Proxy Enabled:
- Port Related Configuration:**

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
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
11	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
12	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

At the bottom of the configuration area, there are 'Save' and 'Reset' buttons.

Object	Description
Snooping Enabled	Enable the Global IGMP Snooping.
Unregistered IPMCv4 Flooding Enabled	Enable unregistered IPMCv4 traffic flooding. The flooding control takes effect only when IGMP Snooping is enabled.

	When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.
IGMP SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
Leave Proxy Enabled	Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
Proxy Enabled	Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
Router Port	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 IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enable the fast leave on the port. Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.
Throttling	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.

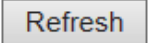
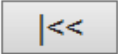


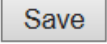
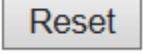
2.3.1.73 VLAN Configuration

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 lets you select the starting point in the VLAN Table.

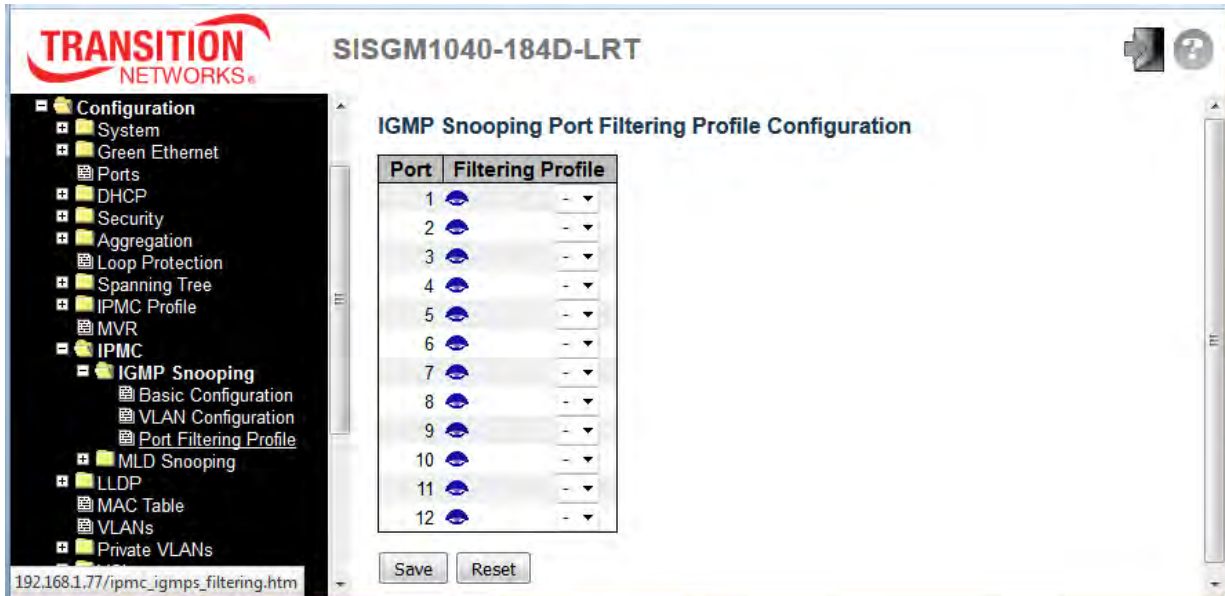
Object	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enabled	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
Querier Election	Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
Querier Address	Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, the switch uses the first available IPv4 management address. Otherwise, the switch uses a pre-defined value. By default, this value will be 192.0.2.1.
Compatibility	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto , Forced IGMPv1 , Forced IGMPv2 , Forced IGMPv3 , default compatibility value is IGMP-Auto.
PRI	Priority of Interface. It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.



	The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.
RV	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255 , default robustness variable value is 2.
QI	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.
QRI	Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of a second, default query response interval is 100 in tenths of seconds (10 seconds).
LLQI (LMQI for IGMP)	Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of a second; default last member query interval is 10 in tenths of a second (1 second).
URI	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

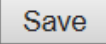
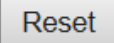
Buttons	
	Refreshes the displayed table starting from the "VLAN" input fields.
	Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.
	Updates the table, starting with the entry after the last entry currently displayed.
	Click to add new IGMP VLAN. 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.

2.3.1.74 Port Filtering Profile

This page lets you configure the IGMP Snooping Port Filtering Profile. The IP MultiCast Profile is used to deploy the access control on IP multicast streams.



Object	Description
Port	The logical port for the settings.
Filtering Profile	Select the IPMC Profile as the filtering condition for the specific port. A Summary of the designated profile will be shown by clicking the view button.
Profile Management Button 	You can inspect the rules of the designated profile by using the  button to List the rules associated with the designated profile.

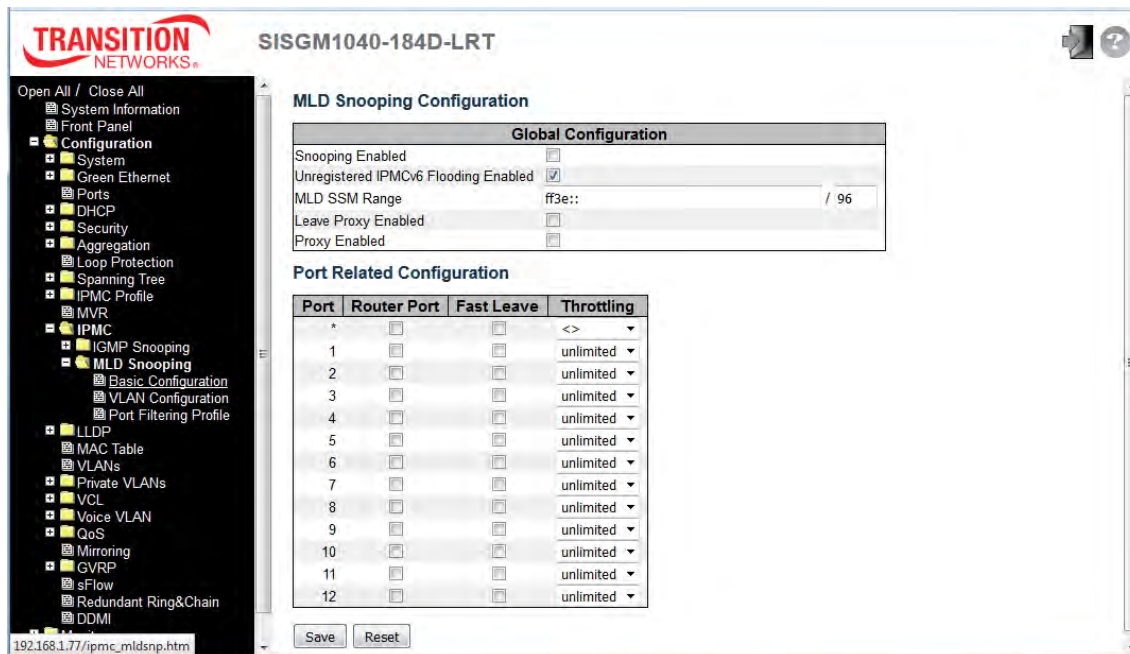
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

2.3.1.75 MLD Snooping

MLD (Multicast Listener Discovery for IPv6) is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

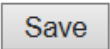

2.3.1.76 Basic Configuration

This page provides MLD Snooping related configuration.



Object	Description
Snooping Enabled	Enable the Global MLD Snooping.
Unregistered IPMCv6 Flooding Enabled	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.
MLD SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
Leave Proxy Enabled	Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
Proxy Enabled	Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Router Port	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 MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enable the fast leave on the port.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

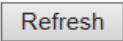
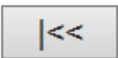



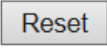
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

2.3.1.77 VLAN Configuration

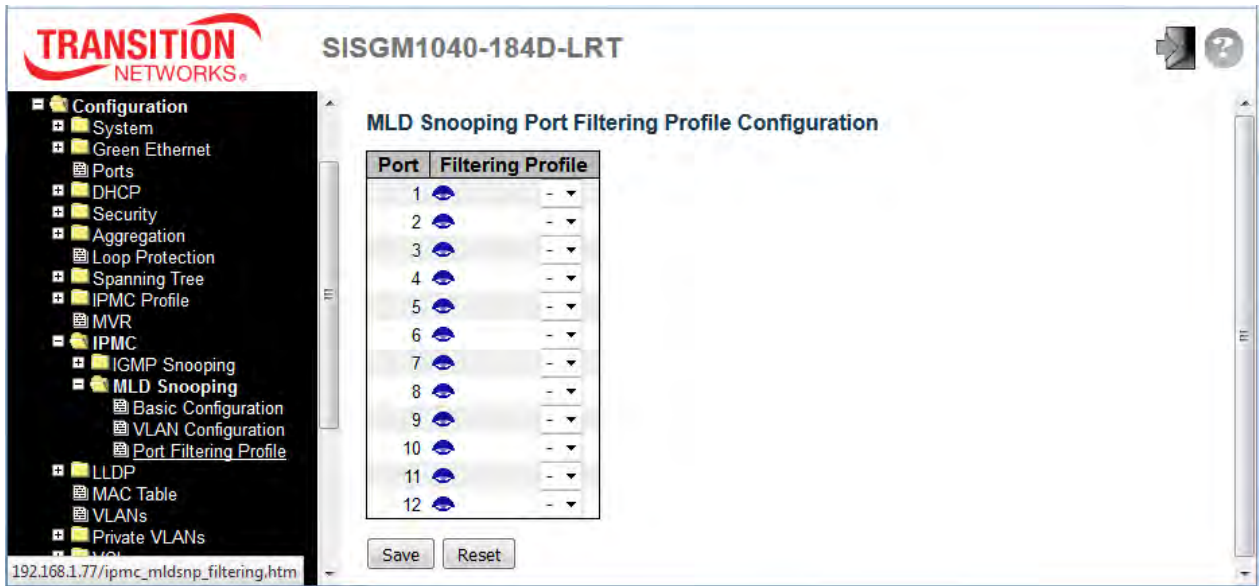
Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields lets you select the starting point in the VLAN Table.



Object	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
VLAN ID	The VLAN ID (VID) of the entry.
MLD Snooping Enabled	Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.
Querier Election	Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.
Compatibility	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 selections are MLD-Auto , Forced MLDv1 , and Forced MLDv2 . The default compatibility value is MLD-Auto.
PRI	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 0 (best effort) to 7 (highest), default interface priority value is 0.
RV	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a link. The allowed range is 1 to 255 , default robustness variable value is 2.
QI	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; the default query interval is 125 seconds.

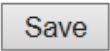
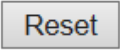
QRI	<p>Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.</p> <p>The allowed range is 0 to 31744 in tenths of a second, default query response interval is 100 in tenths of seconds (10 seconds).</p>
LLQI	<p>Last Listener Query Interval. 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 0 to 31744 in tenths of a second, default last listener query interval is 10 in tenths of seconds (1 second).</p>
URI	<p>Unsolicited Report Interval. 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 0 to 31744 seconds, default unsolicited report interval is 1 second.</p>

Buttons	
	<p>Refreshes the displayed table starting from the "VLAN" input fields.</p>
	<p>Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.</p>
	<p>Updates the table, starting with the entry after the last entry currently displayed.</p>
	<p>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.</p>
	<p>Click to save changes.</p>
	<p>Click to undo any changes made locally and revert to previously saved values.</p>

2.3.1.78 Port Filtering Profile



Object	Description
Port	The logical port for the settings.
Filtering Profile	Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.
Profile Management Button 	You can inspect the rules of the designated profile by using the  button to 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.

2.3.1.79 LLDP

LLDP is an IEEE 802.1ab standard protocol. The Link Layer Discovery Protocol(LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

2.3.1.80 LLDP

This page lets you view and configure the current LLDP port settings.

LLDP Configuration

LLDP Parameters

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

LLDP Port Configuration

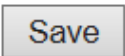

Port	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	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"/>
9	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12	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
LLDP Parameters	
Tx Interval	The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the

	Tx Interval value. Valid values are restricted to 5 - 32768 seconds.
Tx Hold	Each LLDP frame contains information about how long the information in the LLDP frame should be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.
Tx Delay	If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1 - 8192 seconds.
Tx Reinit	When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signalling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.
LLDP Port Parameters	
Port	The switch port number of the logical LLDP port.
Mode	Select LLDP mode. Rx only The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed. Tx only The switch will drop LLDP information received from neighbors, but will send out LLDP information. Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbors. Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbors.
CDP aware	Select CDP awareness. The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled. Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below. CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field. CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table. CDP TLV "Port ID" is mapped to the LLDP "Port ID" field. CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.

	<p>Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.</p> <p>If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.</p> <p>Note: When CDP awareness on a port is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.</p>
Port Descr	Optional TLV: When checked the "port description" is included in LLDP information transmitted.
Sys Name	Optional TLV: When checked the "system name" is included in LLDP information transmitted.
Sys Descr	Optional TLV: When checked the "system description" is included in LLDP information transmitted.
Sys Capa	Optional TLV: When checked the "system capability" is included in LLDP information transmitted.
Mgmt Addr	Optional TLV: When checked the "management address" is included in LLDP information transmitted.

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

2.3.1.81 LLDP-MED

This page lets you configure the LLDP-MED (Link Level Discovery Protocol - Media Endpoint Discovery). This function applies to VoIP devices which support LLDP-MED.

Object	Description
Fast Start Repeat Count	<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</p>



	<p>outgoing LLDPDU 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 increase the possibility of the neighbors receiving the LLDP frame. With Fast start repeat count 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>Note 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>
<p>Coordinates Location</p>	
<p>Latitude</p>	<p>Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator.</p>
<p>Longitude</p>	<p>Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.</p>
<p>Altitude</p>	<p>Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters).</p> <p>Meters: Representing meters of Altitude defined by the vertical datum specified.</p> <p>Floors: 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>
<p>Map Datum</p>	<p>The Map Datum is used for the coordinates given in these options:</p>

	<p>WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.</p> <p>NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian 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>NAD83/MLLW: 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>
Civic Address Location	
Country code	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
State	National subdivisions (state, canton, region, province, prefecture).
County	County, parish, gun (Japan), district.
City	City, township, shi (Japan) - Example: Copenhagen.
City district	City division, borough, city district, ward, chou (Japan).
Block (Neighborhood)	Neighborhood, block.
Street	Street - Example: Poppelvej.
Leading street direction	Leading street direction - Example: N.
Trailing street suffix	Trailing street suffix - Example: SW.
Street suffix	Street suffix - Example: Ave, Platz.
House no.	House number - Example: 21.
House no. suffix	House number suffix - Example: A, 1/2.
Landmark	Landmark or vanity address - Example: Columbia University.
Additional location info	Additional location info - Example: South Wing.
Name	Name (residence and office occupant) - Example: Flemming Jahn.
Zip code	Postal/zip code - Example: 2791.
Building	Building (structure) - Example: Low Library.
Apartment	Unit (Apartment, suite) - Example: Apt 42.
Floor	Floor - Example: 4.
Room no.	Room number - Example: 450F.
Place type	Place type - Example: Office.
Postal community name	Postal community name - Example: Leonia.
P.O. Box	Post office box (P.O. BOX) - Example: 12345.

Additional code	Additional code - Example: 1320300003.
Emergency Call Service	
Emergency Call Service	Emergency Call Service 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.
Policies	
Delete	Check to delete the policy. It will be deleted during the next save.
Policy ID	ID for the policy. This is auto generated and will be used when selecting the policies that will be mapped to the specific ports.
Application Type	<p>Intended use of the application types:</p> <ol style="list-style-type: none"> 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. Voice Signalling (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 Voice application policy. Guest Voice - 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. Guest Voice Signalling (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 Guest Voice application policy. Softphone Voice - 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.

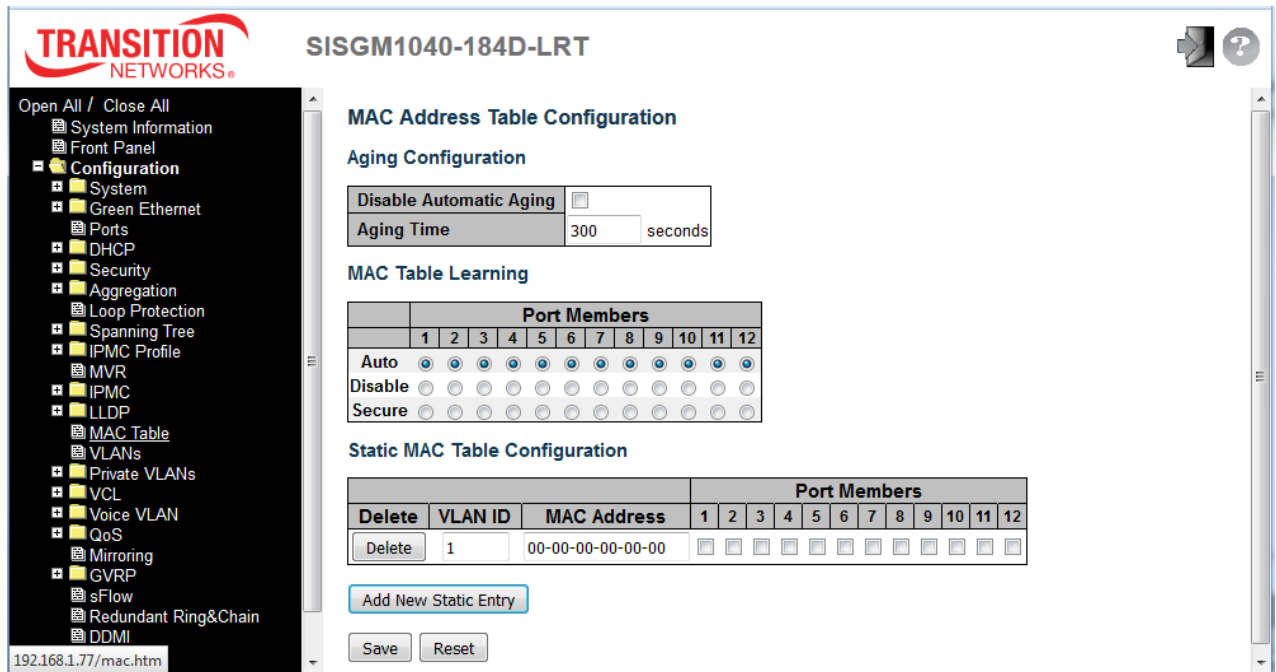
	<p>6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.</p> <p>7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming 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.</p> <p>8. Video Signalling (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 Video Conferencing application policy.</p>
Tag	<p>Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN.</p> <p>Untagged 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>Tagged 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>
VLAN ID	VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.
L2 Priority	L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority 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.
DSCP	DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP 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.
Adding a new policy	Click the Add New Policy button to add a new policy. Specify the Application type , Tag , VLAN ID , L2 Priority and DSCP for the new policy. Click "Save". The number of

	policies supported is 32.
Port Policies Configuration	
Port	The port number to which the configuration applies.
Policy Id	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.

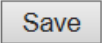
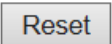
2.3.1.82 MAC Table

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. Click the **Add New Static Entry** button to add a new entry to the static MAC table.



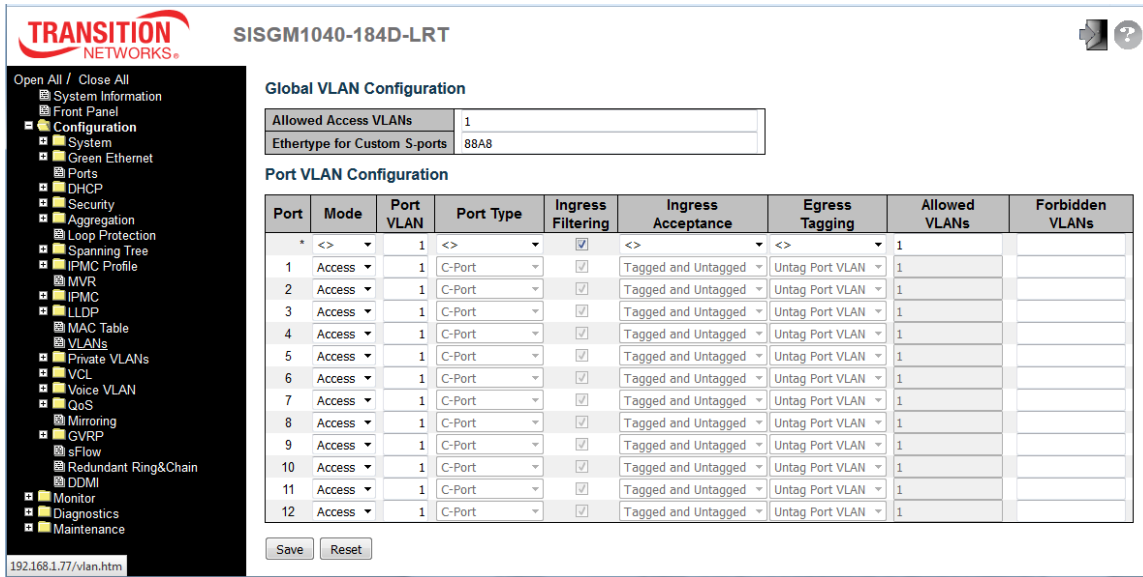
Object	Description
Aging Configuration	
Disable Automatic Aging	Disable the automatic aging of dynamic entries by ticking the item.
Aging Time	Enter a value in seconds. The allowed range is 10 to 1000000 seconds.
MAC Table Learning	
Auto	Learning is done automatically as soon as a frame with unknown SMAC is received.
Disable	No learning is done.
Secure	Only static MAC entries are learned, all other frames are dropped. Note: 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.

Static MAC Table Learning	
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Adding a New Static Entry	<p>Click the  button to add a new entry to the static MAC table.</p> <p>Specify the VLAN ID, MAC address, and port members for the new entry.</p> <p>Click "Save" when done.</p>

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

2.3.1.83 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.

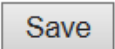
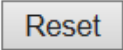


Object	Description
Global VLAN Configuration	
Allowed Access VLANs	This field shows the allowed Access VLANs, i.e. it only affects ports configured as Access ports. Ports in other modes are members of all VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be 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: <code>1, 10-13, 200, 300</code> . Spaces are allowed in between the delimiters.
Ethertype for Custom S-ports	This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.
Port VLAN Configuration	
Port	This is the logical port number of this row.
Mode	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.

	<p><u>Access:</u> 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"> • Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1 • Accepts untagged and C-tagged frames • Discards all frames that are not classified to the Access VLAN • On egress all frames classified to the Access VLAN are transmitted untagged. Other (dynamically added VLANs) are transmitted tagged <p><u>Trunk:</u> 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"> • By default, a trunk port is member of all VLANs (1-4095) • The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs • Frames classified to a VLAN that the port is not a member of are discarded • 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 • Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress <p><u>Hybrid:</u> Hybrid ports resemble trunk ports in many ways, but add 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"> • Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware • Ingress filtering can be controlled. • Ingress acceptance of frames and configuration of egress tagging can be configured independently.
<p>Port VLAN</p>	<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</p>

	<p>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 Egress Tagging 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>
Port Type	<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>Unaware: 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>C-Port: 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>S-Port: 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>S-Custom-Port: On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports 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>
Ingress Filtering	<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 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>
Ingress Acceptance	<p>Hybrid ports allow for changing the type of frames that are accepted on ingress.</p> <p>Tagged and Untagged: Both tagged and untagged frames are accepted.</p>

	<p>Tagged Only: Only tagged frames are accepted on ingress. Untagged frames are discarded.</p> <p>Untagged Only: Only untagged frames are accepted on ingress. Tagged frames are discarded.</p>
Egress Tagging	<p>Ports in Trunk and Hybrid mode may control the tagging of frames on egress.</p> <p>Untag Port VLAN: Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.</p> <p>Tag All: All frames, whether classified to the Port VLAN or not, are transmitted with a tag.</p> <p>Untag All: 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>
Allowed VLANs	<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 Enabled VLANs 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>
Forbidden VLANs	<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 Enabled VLANs 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.

2.3.1.84 Private VLANs

In a private VLAN, PVLANS provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

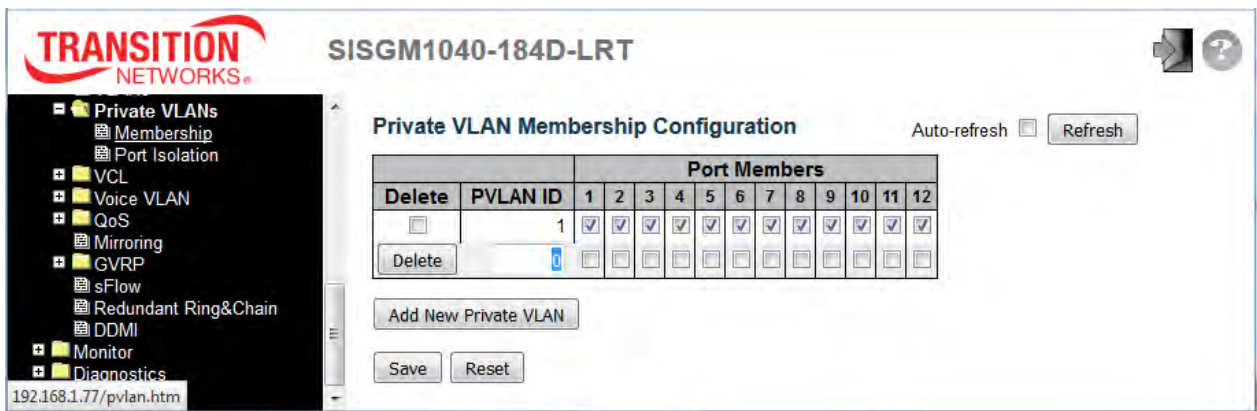
2.3.1.85 Membership

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.

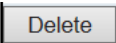
A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

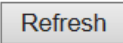
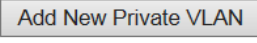
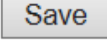
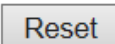
A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

Click the **Add New Private VLAN** button to add a row to the table, enter a PVLAN ID, and then select Port Members.



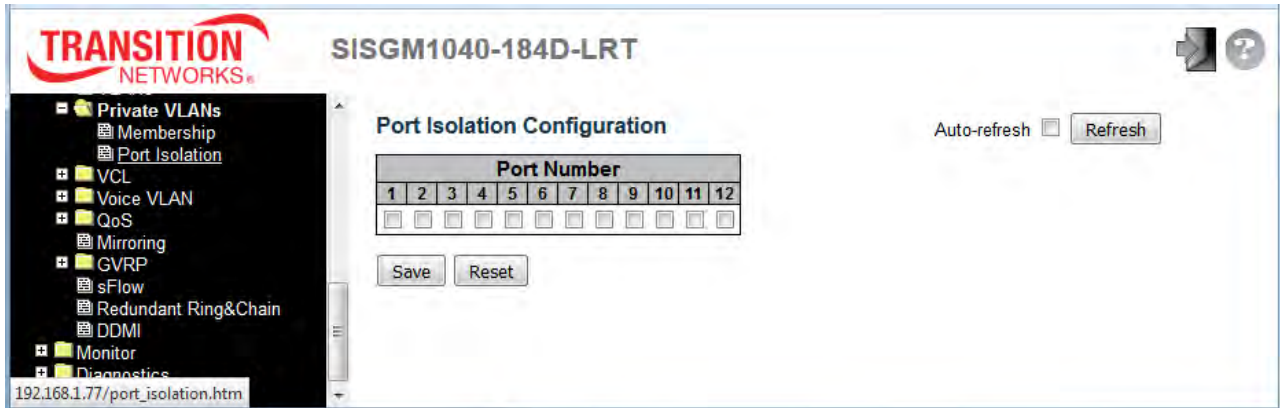
Object	Description
Delete	To delete a private VLAN entry, check this box. The entry will be deleted during the next save.
PVLAN ID	Indicates the ID of this particular private VLAN.
Port Members	A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, 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.
Adding a New Private VLAN	<p>Click the Add New Private VLAN button to add a new private VLAN ID.</p> <p>An empty row is added to the table, and the private VLAN can be configured as needed.</p> <p>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.

2.3.1.86 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.



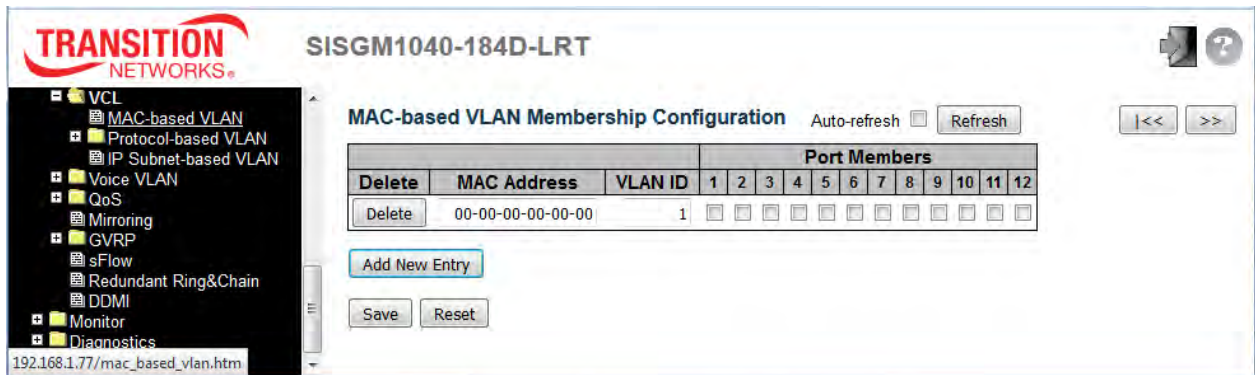
Object	Description
Port Number	<p>A checkbox is provided for each port of a private VLAN.</p> <p>When checked, port isolation is enabled on that port.</p> <p>When unchecked, port isolation is disabled on that port.</p> <p>By default, port isolation is disabled on all ports.</p>

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

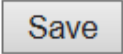
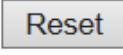
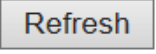
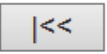

2.3.1.87 VCL

2.3.1.88 MAC-based VLAN

MAC-based VLAN entries can be configured here. This page lets you add and delete MAC-based VLAN entries and assign the entries to different ports. This page shows only static entries. Click the **Add New Entry** button to add a row to the table, enter a PVLAN ID, and then select Port Members.



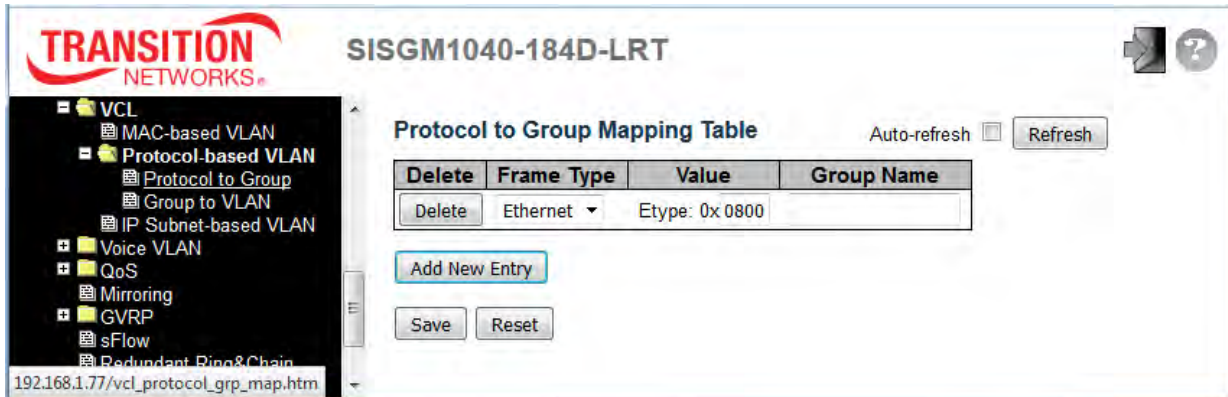
Object	Description
Delete	To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted.
MAC Address	Indicates the MAC address.
VLAN ID	Indicates the VLAN ID.
Port Members	A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in 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.
Adding a New MAC-based VLAN	<p>Click Add New Entry 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 1 through 4095.</p> <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 Delete button can be used to undo the addition of new MAC-based VLANs. 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 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.

2.3.1.89 Protocol-based VLAN

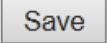
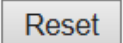

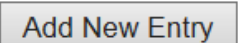
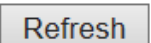
2.3.1.90 Protocol to Group

This page lets you 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.



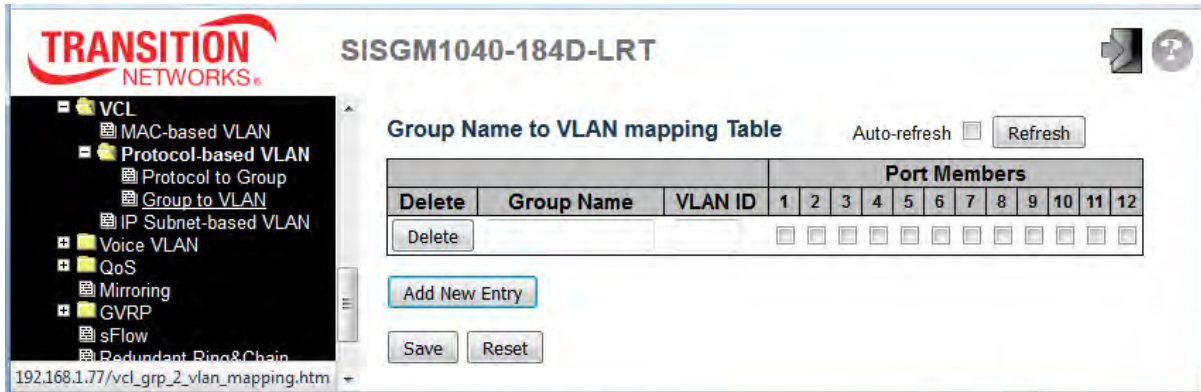
Object	Description
Delete	To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.
Frame Type	<p>Frame Type can have one of the following values:</p> <p>Ethernet: Match EtherType frames.</p> <p>LLC: Match (LLC) frames.</p> <p>SNAP: Match (SNAP) frames.</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>
Value	<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>For Ethernet: 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>For LLC: Valid value in this case is comprised of two different sub-values.</p> <p>a. DSAP: 1-byte long string (0x00-0xff)</p>

	<p>b. SSAP: 1-byte long string (0x00-0xff)</p> <p>For SNAP: Valid value in this case also is comprised of two different sub-values.</p> <p>a. OUI: 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. PID: 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>
Group Name	<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>Note: special character and underscore (_) are not allowed.</p>

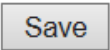
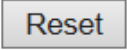
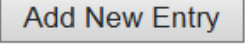

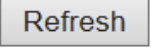
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.
	The button can be used to undo the addition of new entry. Up to 128 Protocol to Group are supported.
	Click to add a new entry in mapping table.
Auto-refresh <input type="checkbox"/>	Check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

2.3.1.91 Group to VLAN

This page lets you map an already configured Group Name to a VLAN for the switch.

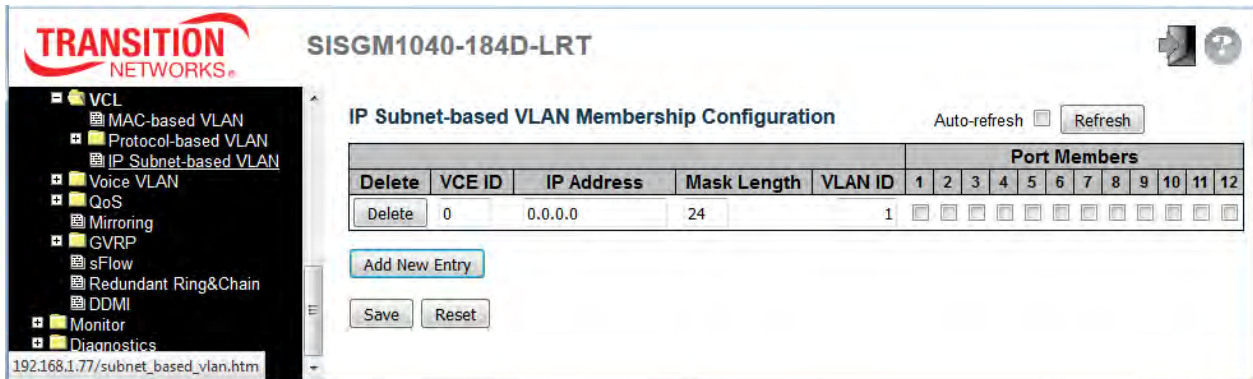


Object	Description
Delete	To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save.
Group Name	A valid Group Name is a string at the most 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers(0-9), no special 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.
VLAN ID	Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.
Port Members	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.
Adding a New Group to VLAN mapping entry	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 1 through 4095 . The <input type="button" value="Delete"/> button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings is limited to 64.

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. Valid values for a VLAN ID are 1 - 4095 .
	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 every 3 seconds.
	Click to refresh the page immediately.




2.3.1.92 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
Delete	To delete an IP subnet-based VLAN entry, check this box and press save. The entry will be deleted.
VCE ID	Indicates the index of the entry. It is user configurable. Its 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.
IP Address	Indicates the IP address.
Mask Length	Indicates the network mask length.
VLAN ID	Indicates the VLAN ID. VLAN ID can be changed for the existing entries.
Port Members	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.

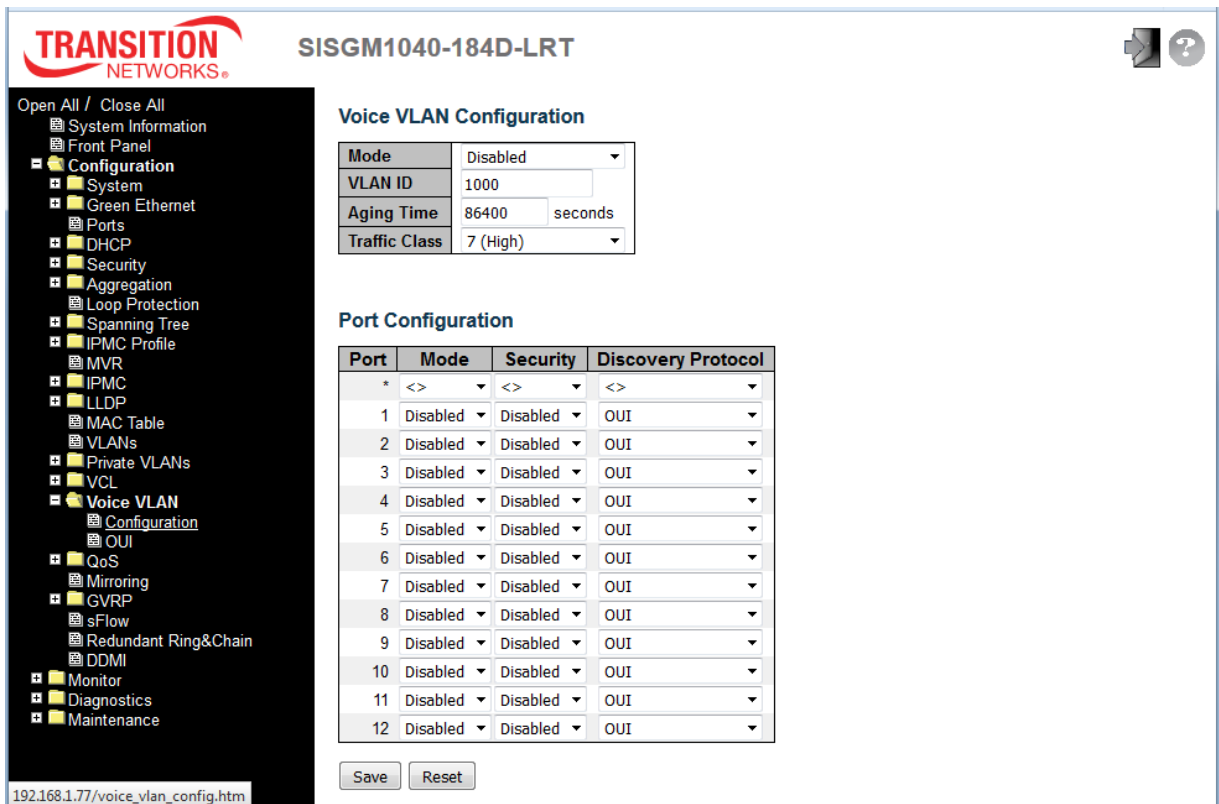
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

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

2.3.1.93 Voice VLAN

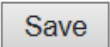
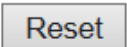
2.3.1.94 Voice VLAN Configuration

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 through its own GUI.



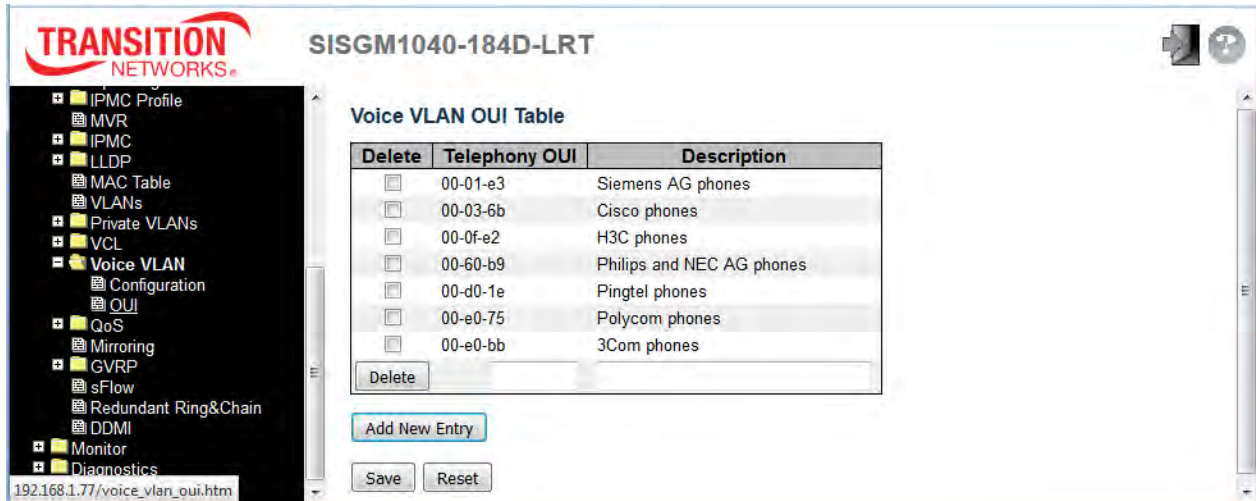
Object	Description
Mode	Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are: Enabled: Enable Voice VLAN mode operation. Disabled: Disable Voice VLAN mode operation.
VLAN ID	Indicates the 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 1 to 4095.

Aging Time	Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 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.
Traffic Class	Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.
Mode	Indicates the Voice VLAN port mode. Possible port modes are: Disabled : Disjoin from Voice VLAN. Auto : Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically. Forced : Force join to Voice VLAN.
Security	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. Possible port modes are: Enabled : Enable Voice VLAN security mode operation. Disabled : Disable Voice VLAN security mode operation.
Discovery Protocol	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: OUI : Detect telephony device by OUI address. LLDP : Detect telephony device by LLDP. Both : Both OUI and LLDP.

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

2.3.1.95 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 the OUI (Organizationally Unique Identifier) process.

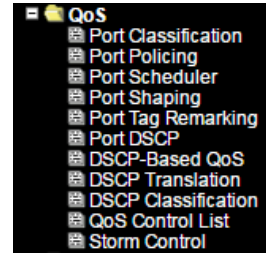


Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Telephony OUI	A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).
Description	The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

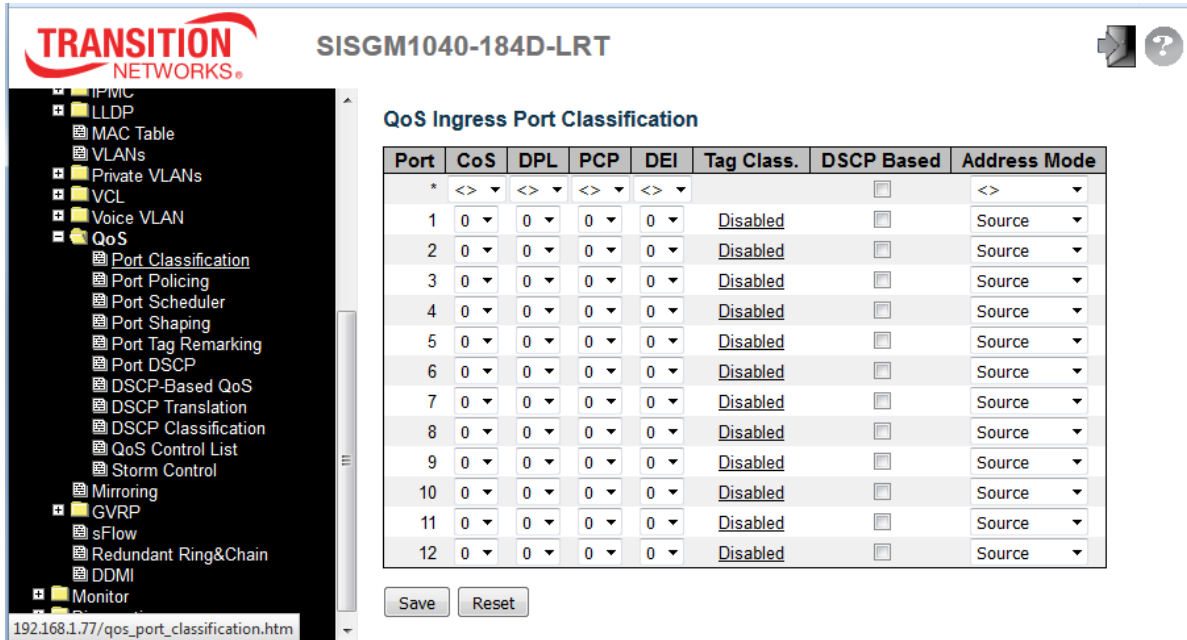
Buttons	
	Click to add a new access management entry.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

2.3.1.96 QoS

2.3.1.97 Port Classification

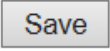
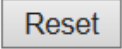


This page lets you configure the basic QoS Ingress Classification settings for all switch ports.



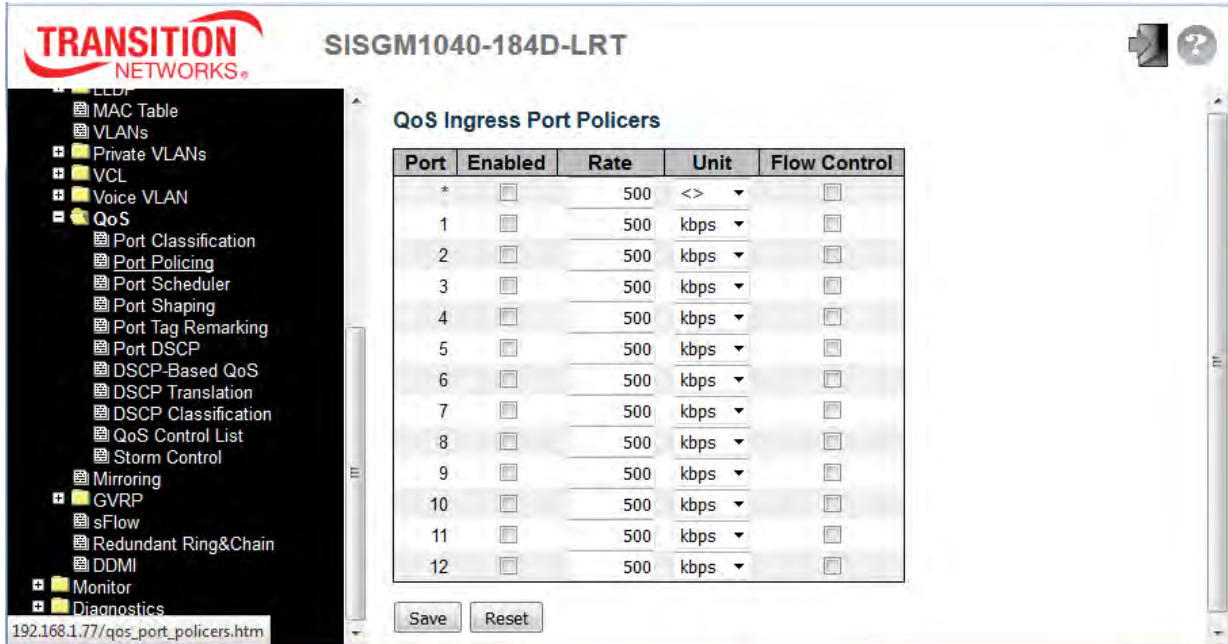
Object	Description
Port	The port number for which the configuration below applies.
CoS	<p>Controls the default class of service (CoS). All frames are classified to a CoS. There is a one-to-one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority.</p> <p>If the port is VLAN 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. The classified CoS can be overruled by a QCL entry.</p> <p>Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.</p>
DPL	Controls the default drop precedence level. All frames are classified to a drop precedence level. 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.

	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. The classified DPL can be overruled by a QCL entry.
PCP	Controls the default PCP value. All frames are classified to a PCP value. 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.
DEI	Controls the default DEI value. DEI (Drop Eligible Indicator) is a 1-bit field in the VLAN tag. All frames are classified to a DEI value. 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.
Tag Class.	Shows the classification mode for tagged frames on this port. Disabled: Use default CoS and DPL for tagged frames. Enabled: Use mapped versions of PCP and DEI for tagged frames. Click on the linked mode (<u>Enabled</u> or <u>Disabled</u>) in order to configure the mode and/or mapping. Note: This setting has no affect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.
DSCP Based	Click to Enable DSCP Based QoS Ingress Port Classification.
Address Mode	The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. Allowed values are: Source: Enable SMAC/SIP matching. Destination: Enable DMAC/DIP matching.

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

2.3.1.98 Port Policing

This page lets you configure the Policer settings for all switch ports.



Object	Description
Port	The port number for which the configuration below applies.
Enabled	Controls whether the policer is enabled on this switch port.
Rate	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".
Unit	Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps. The default value is "kbps".
Flow Control	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.

2.3.1.99 Port Scheduler

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

Port	Mode	Weight				
		Q0	Q1	Q2	Q3	Q4
1	Strict Priority	-	-	-	-	-
2	Strict Priority	-	-	-	-	-
3	Strict Priority	-	-	-	-	-
4	Strict Priority	-	-	-	-	-
5	Strict Priority	-	-	-	-	-
6	Strict Priority	-	-	-	-	-
7	Strict Priority	-	-	-	-	-
8	Strict Priority	-	-	-	-	-
9	Strict Priority	-	-	-	-	-
10	Strict Priority	-	-	-	-	-
11	Strict Priority	-	-	-	-	-
12	Strict Priority	-	-	-	-	-

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

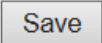
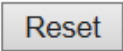
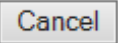
The QoS Egress Port Scheduler and Shapers for Port 2 are shown below. Note that the default Scheduler Mode is changed from the default (Strict Priority) to Weighted priority for Port 2.

Queue Shaper				Queue Scheduler		Port Shaper		
Enable	Rate	Unit	Excess	Weight	Percent	Enable	Rate	Unit
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>	500	kbps

QoS Egress Port Scheduler and Shapers Parameters

This page lets you configure the Scheduler and Shapers for a specific port. The displayed settings are described below.

Object	Description
Scheduler Mode	Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.
Queue Shaper Enable	Controls whether the queue shaper is enabled for this queue on this switch port.
Queue Shaper Rate	Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps".
Queue Shaper Unit	Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".
Queue Shaper Excess	Controls whether the queue is allowed to use excess bandwidth.
Queue Scheduler Weight	Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
Queue Scheduler Percent	Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
Port Shaper Enable	Controls whether the port shaper is enabled for this switch port.
Port Shaper Rate	Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps".
Port Shaper Unit	Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons	
	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 previous page.

2.3.1.100 Port Shaping

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

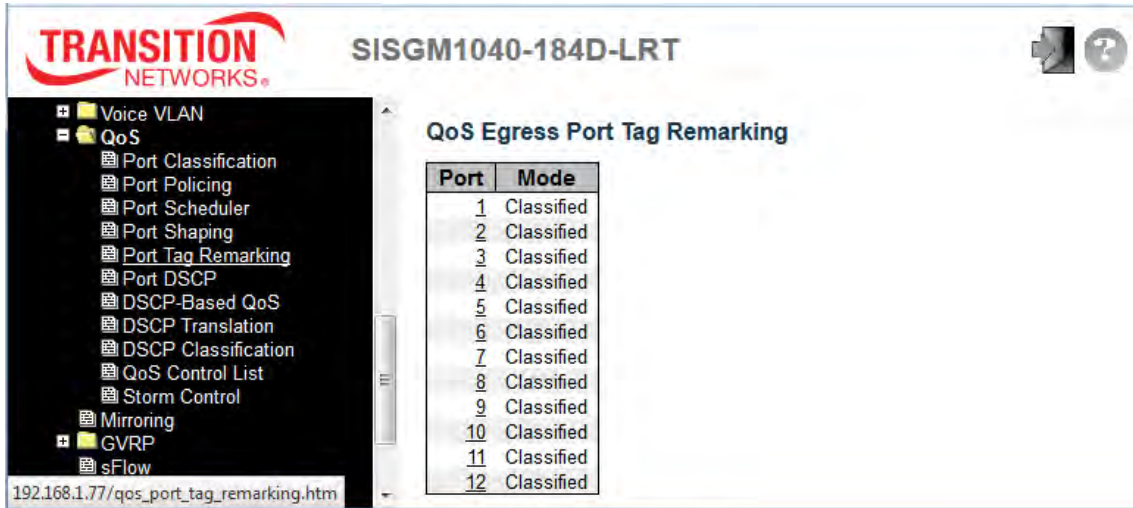
Port	Shapers							Port	
	Q0	Q1	Q2	Q3	Q4	Q5	Q6		Q7
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	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
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
11	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
12	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

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

See the previous section for “QoS Egress Port Scheduler and Shapers” parameter descriptions.

2.3.1.101 Port Tag Remarking

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



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

Click on a linked port number to configure tag remarking (for Port 2 in the example below).



2.3.1.102 Port DSCP

This page lets you configure the basic QoS Port DSCP Configuration settings for all switch ports.

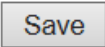
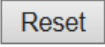
The screenshot displays the 'QoS Port DSCP Configuration' page. On the left is a navigation tree with categories like QoS, Monitor, and System. The main area shows a table for configuring DSCP settings for ports 1-12. The table has columns for 'Port', 'Ingress' (with sub-columns 'Translate' and 'Classify'), and 'Egress' (with sub-column 'Rewrite').

Port	Ingress		Egress
	Translate	Classify	Rewrite
1	<input type="checkbox"/>	Disable	Disable
2	<input type="checkbox"/>	DSCP=0	Enable
3	<input type="checkbox"/>	Selected	Remap DP Unaware
4	<input type="checkbox"/>	All	Remap DP Aware
5	<input type="checkbox"/>	Disable	Disable
6	<input type="checkbox"/>	Disable	Disable
7	<input type="checkbox"/>	Disable	Disable
8	<input type="checkbox"/>	Disable	Disable
9	<input type="checkbox"/>	Disable	Disable
10	<input type="checkbox"/>	Disable	Disable
11	<input type="checkbox"/>	Disable	Disable
12	<input type="checkbox"/>	Disable	Disable

At the bottom of the table are 'Save' and 'Reset' buttons. The URL at the bottom of the browser window is https://192.168.1.77/qos_port_dscp_config.htm.

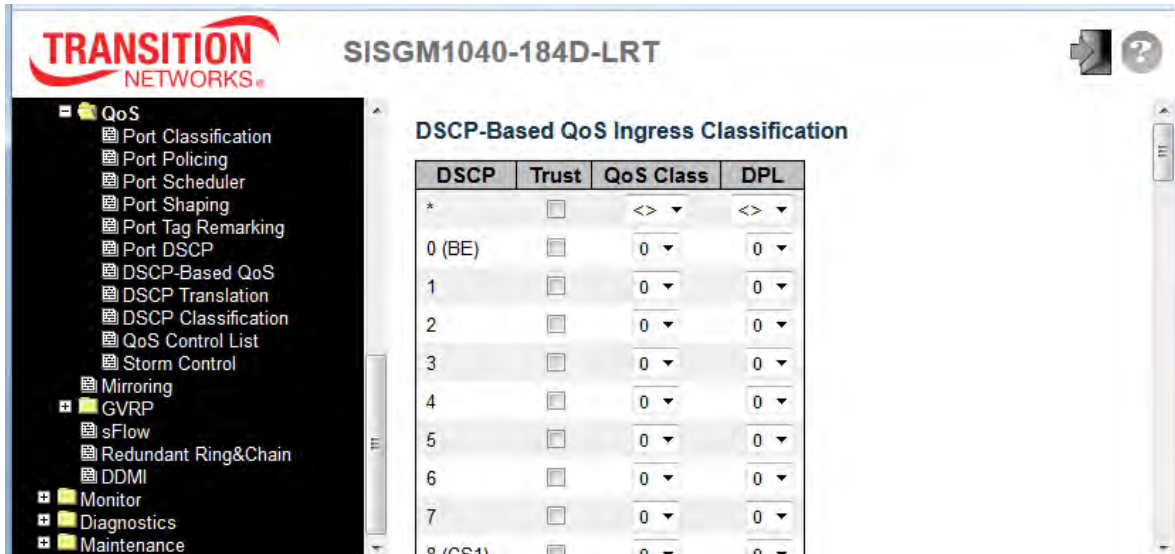
Object	Description
Port	The Port column shows the list of ports for which you can configure DSCP ingress and egress settings.
Ingress	In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: Translate Classify
Translate	To enable Ingress Translation click the checkbox.
Classify	Classification for a port have one of four different values. Disable : No Ingress DSCP Classification. DSCP=0 : Classify if incoming (or translated if enabled) DSCP is 0. Selected : Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP. All : Classify all DSCP.
Egress Rewrite	Port Egress Rewriting can be one of these values: Disable : No Egress rewrite. Enable : Rewrite enabled without remapping. Remap DP Unaware : DSCP from analyzer is remapped and frame is remarked with remapped

	<p>DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation > Egress Remap DP0' table.</p> <p>Remap DP Aware: 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> Egress Remap DP0' table or from the 'DSCP Translation > Egress Remap DP1' table.</p>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

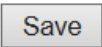
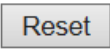
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

2.3.1.103 DSCP-Based QoS

This page lets you configure the basic QoS DSCP-based QoS Ingress Classification settings.

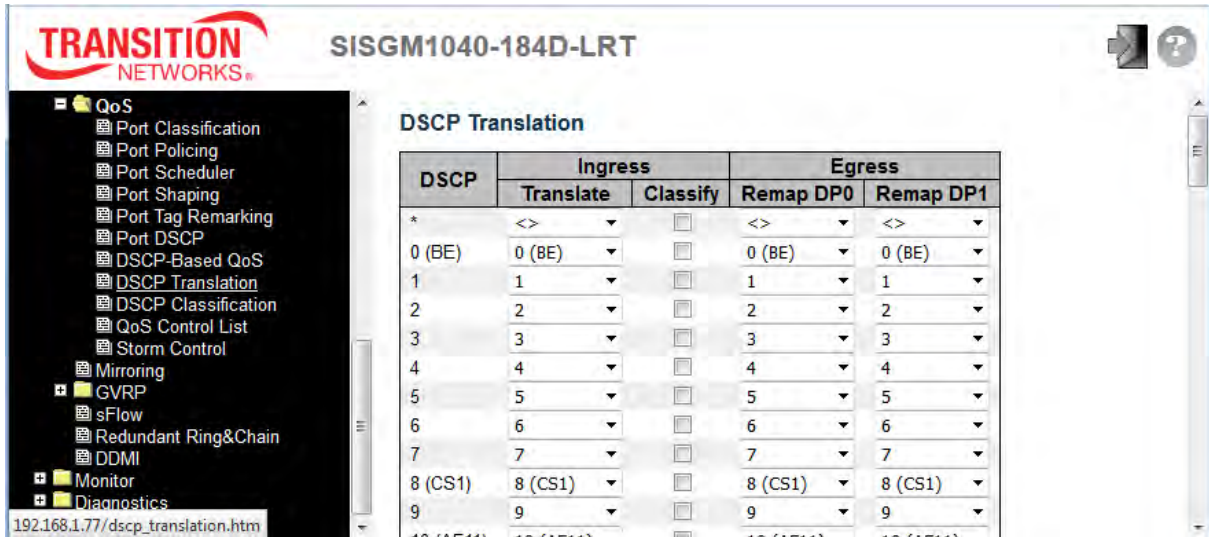


Object	Description
DSCP	Maximum number of supported DSCP values is 64.
Trust	Controls whether a specific DSCP value is trusted. Only frames with <u>trusted</u> DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with <u>untrusted</u> DSCP values are treated as a non-IP frame.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



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

2.3.1.104 DSCP Translation

This page lets you configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.

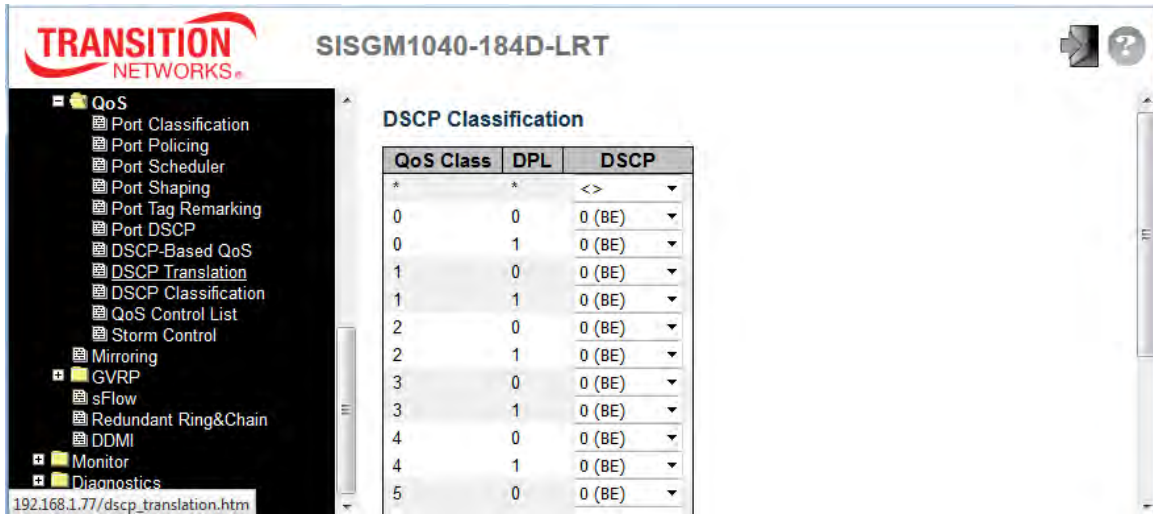


Object	Description
DSCP	Maximum number of supported DSCP values is 64; valid DSCP value ranges from 0 to 63.
Ingress	Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. The two configuration parameters for DSCP Translation (Translate and Classify) are described below.
Translate	DSCP at Ingress side can be translated to any of (0-63) DSCP values.
Classify	Click to enable Classification at Ingress side.
Egress	There are the following configurable parameters for Egress side: Remap DP0 Controls the remapping for frames with DP level 0. Remap DP1 Controls the remapping for frames with DP level 1.
Remap DP0	From the menu, select the DSCP value which you want to remap. DSCP value ranges from 0 to 63.
Remap DP1	From the menu, select the DSCP value which you want to remap. DSCP value ranges from 0 to 63.

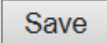
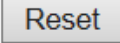
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

2.3.1.105 DSCP Classification

This page lets you configure the mapping of QoS class and Drop Precedence Level to DSCP value.

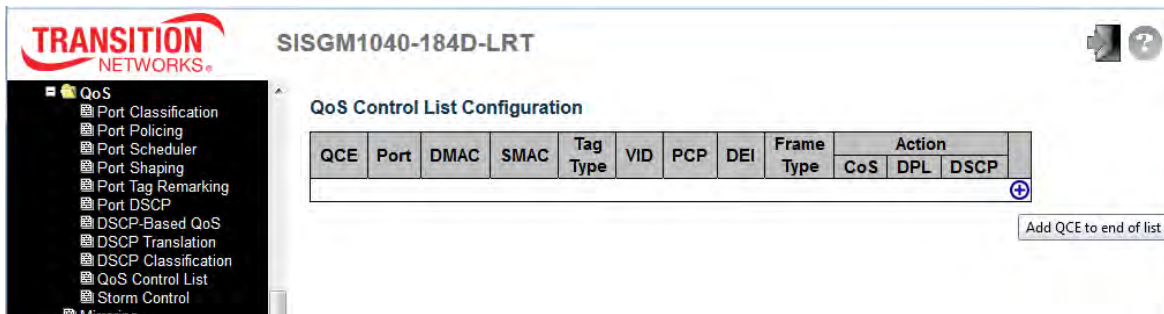


Object	Description
QoS Class	Actual QoS class.
DPL	Actual Drop Precedence Level.
DSCP	Select the classified DSCP value (0-63).







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

2.3.1.106 QoS Control List

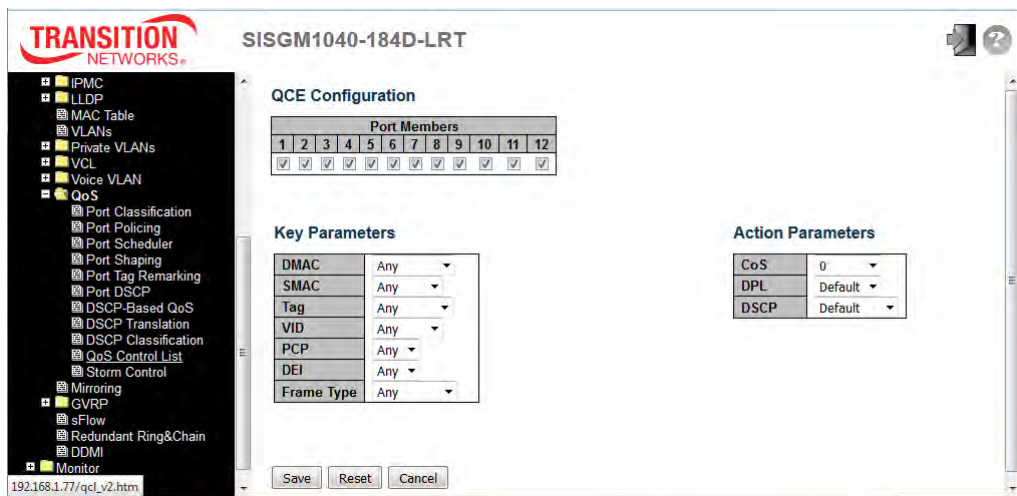
This page shows the QoS Control List (QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is **256** on each switch. Click the plus sign (+) to add a new QCE to the list.



Object	Description
QCE	Indicates the QCE id.
Port	Indicates the list of ports configured with the QCE.
DMAC	Indicates the destination MAC address. Possible values are: Any : Match any DMAC. Unicast : Match unicast DMAC. Multicast : Match multicast DMAC. Broadcast : Match broadcast DMAC. The default value is 'Any'.
SMAC	Match specific source MAC address or 'Any'. If a port is configured to match on DMAC/DIP, this field indicates the DMAC.
Tag Type	Indicates tag type. Possible values are: Any : Match tagged and untagged frames. Untagged : Match untagged frames. Tagged : Match tagged frames. The default value is 'Any'.
VID	Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'
PCP	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'.
DEI	Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.

<p>Frame Type</p>	<p>Indicates the type of frame. Possible values are:</p> <p>Any: Match any frame type.</p> <p>Ethernet: Match EtherType frames.</p> <p>LLC: Match (LLC) frames.</p> <p>SNAP: Match (SNAP) frames.</p> <p>IPv4: Match IPv4 frames.</p> <p>IPv6: Match IPv6 frames.</p>
<p>Action</p>	<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>CoS: Classify Class of Service.</p> <p>DPL: Classify Drop Precedence Level.</p> <p>DSCP: Classify DSCP value.</p>
<p>Modification Buttons</p>	<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>

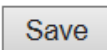
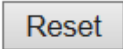
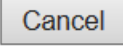
The QCE page can display a variety of fields based on the parameters selected.





The QCE page fields are described below.

Object	Description
Port Members	Check the checkbox to include the port in the QCL entry. By default all ports are included.
Key parameters	<p>Key configuration is described as below:</p> <p>DMAC Destination MAC address: Values are 'Unicast', 'Multicast', 'Broadcast' or 'Any'.</p> <p>SMAC 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>Tag Value of Tag field can be 'Untagged', 'Tagged' or 'Any'.</p> <p>VID 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>PCP 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>DEI Valid value of DEI can be '0', '1' or 'Any'.</p> <p>Frame Type Frame Type can have any of the following values:</p> <p>Any: Allow all types of frames.</p> <p>EtherType: Ether Type Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'.</p> <p>LLC: SSAP Address Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'.</p> <p>DSAP Address Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'.</p> <p>Control Valid Control field can vary from 0x00 to 0xFF or 'Any'.</p> <p>SNAP: PID Valid PID (a.k.a Ether Type) can be 0x0000-0xFFFF or 'Any'.</p> <p>IPv4: Protocol IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.</p> <p>Source IP 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>IP Fragment IPv4 frame fragmented option: 'Yes', 'No' or 'Any'.</p> <p>DSCP 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>Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.</p> <p>Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.</p>





	<p>IPv6: Protocol IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.</p> <p>Source IP 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>DSCP 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>Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.</p> <p>Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.</p>
Action Parameters	<p>CoS Class of Service: (0-7) or 'Default'.</p> <p>DP Drop Precedence Level: (0-1) or 'Default'.</p> <p>DSCP: (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.


SISGM1040-184D-LRT


- 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
- Redundant Ring&Chain

QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action			
									CoS	DPL	DSCP	
1	2-10	Unicast	Any	Any	Any	Any	Any	Any	0	Default	Default	
2	All	Any	Any	Any	Any	Any	Any	Ethernet	0	Default	Default	
3	All	Unicast	Any	Untagged	Any	Any	Any	LLC	0	0	0 (BE)	
4	All	Any	Any	Untagged	Any	Any	Any	IPv4	0	Default	Default	


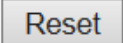
2.3.1.107 Storm Control

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

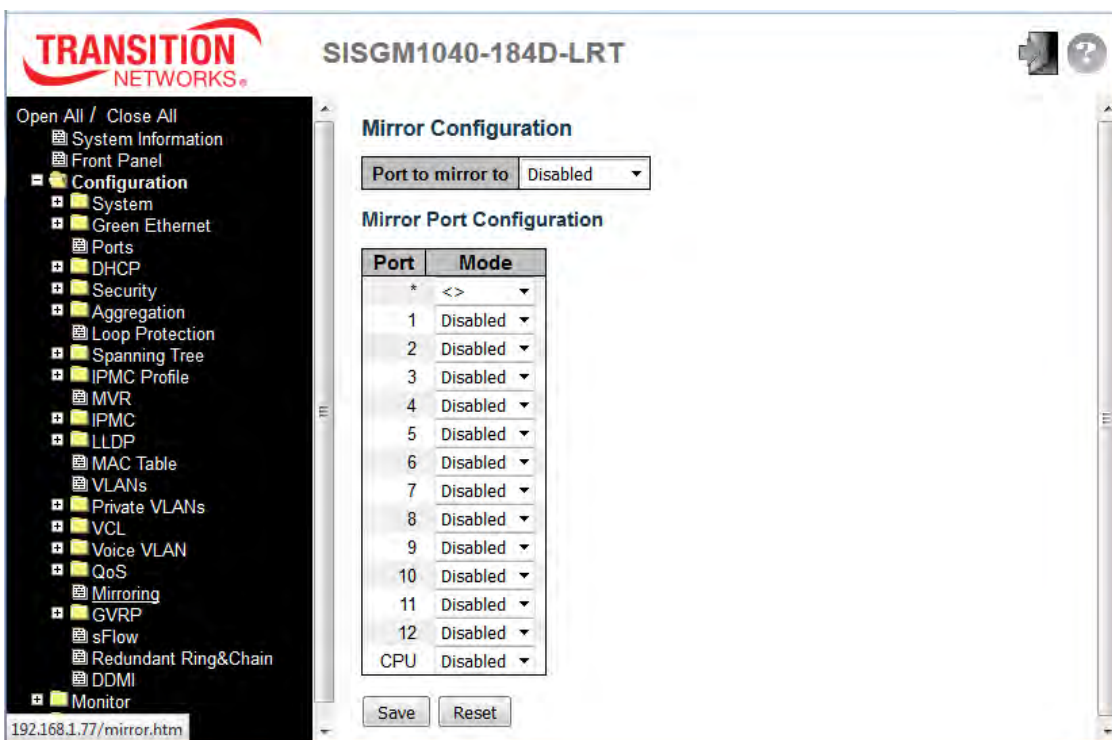
Buttons	
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

2.3.1.108 Mirror

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 to	Port to mirror also known as the mirror port . Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. Disabled disables mirroring.
Port	The logical port for the settings contained in the same row.
Mode	Select the mirror mode. Rx only Frames received on this port are mirrored on the mirror port . Frames transmitted are not mirrored. Tx only Frames transmitted on this port are mirrored on the mirror port . Frames received are not mirrored.

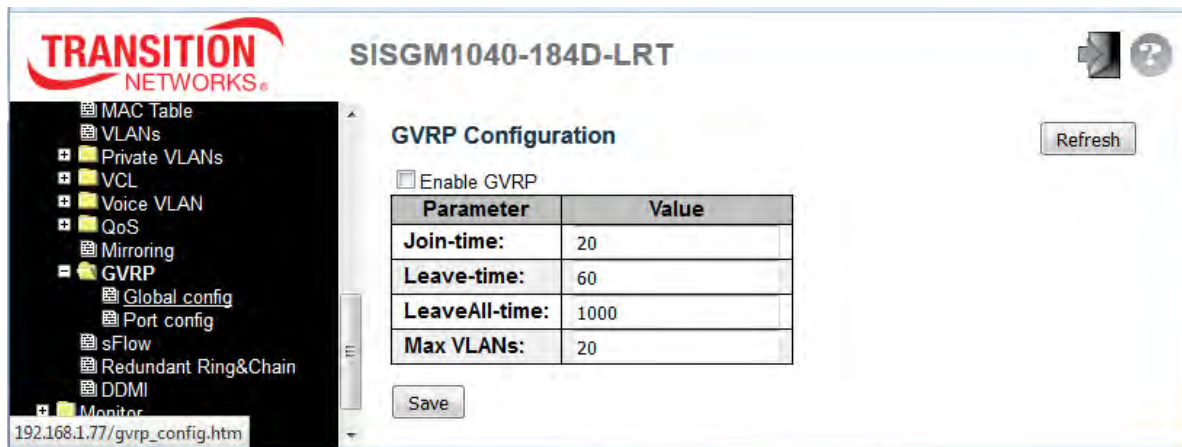
	<p>Disabled Neither frames transmitted nor frames received are mirrored.</p> <p>Enabled Frames received and frames transmitted are mirrored on the mirror port.</p> <p>Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror the mirror port Tx frames. So mode for the selected mirror port is limited to Disabled or Rx only.</p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Buttons	
<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.

2.3.1.109 GVRP

2.3.1.110 GVRP Global Config

This page lets you configure the basic GVRP settings for all switch ports. GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data.

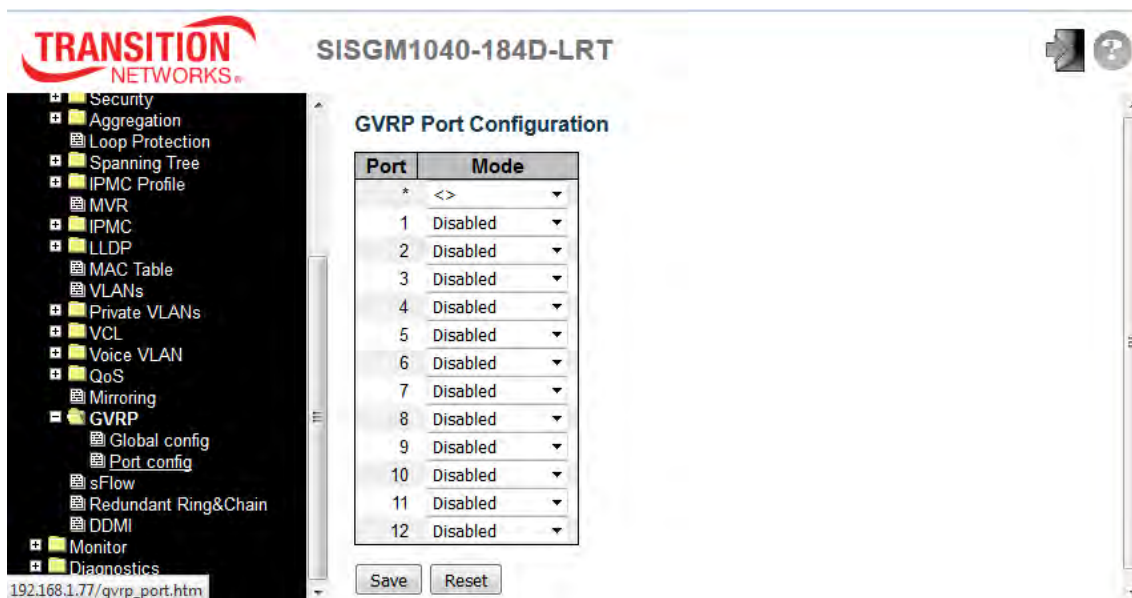


Object	Description
Enable GVRP	Check the box to enable GVRP globally.
GVRP Protocol timers	<p>Join-time is a value in the range 1-20 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 20.</p> <p>Leave-time is a value in the range 60-300 in the units of centi seconds, 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>
Max VLANs	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.
<input type="button" value="Refresh"/>	Click to refresh the page immediately. Note that unsaved changes will be lost.

2.3.1.111 GVRP Port Config

This page lets you enable a port for GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol).



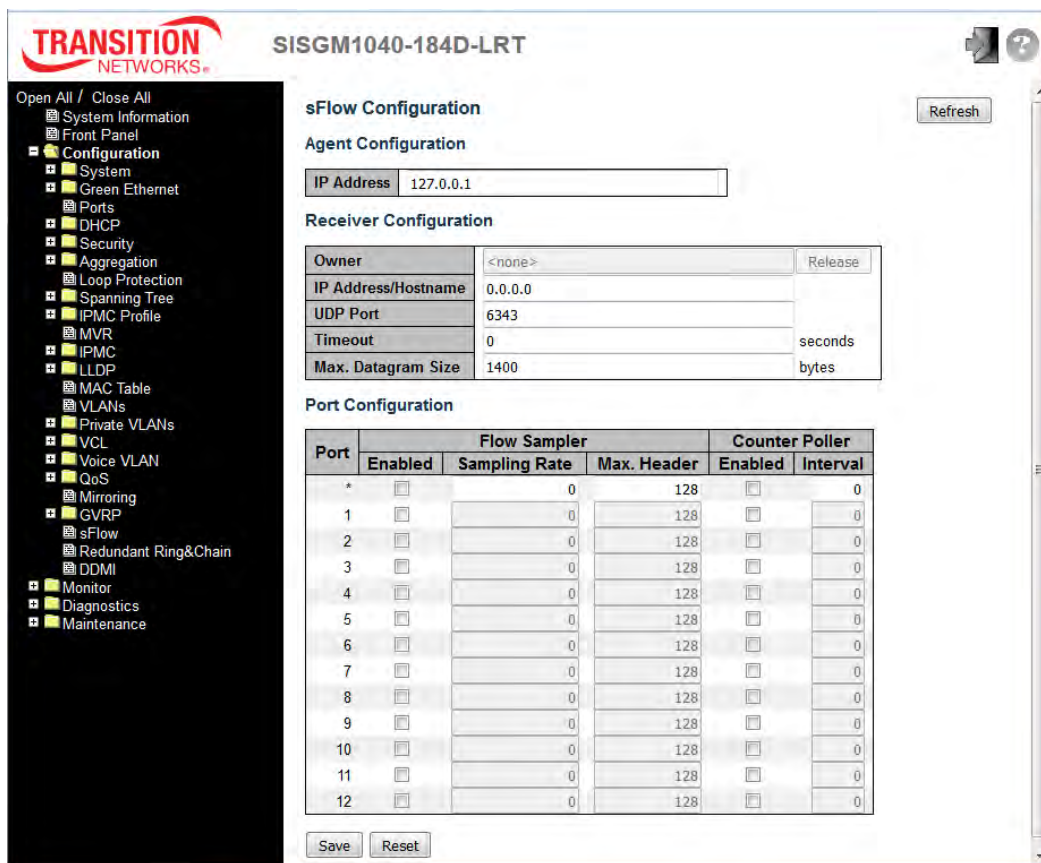
Object	Description
Mode	Enable a port for GVRP; the default is Disabled.

Buttons	
<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.

2.3.1.112 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.

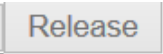

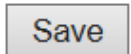
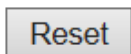
sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector. Additional information can be found at <http://sflow.org>.



Object	Description
Agent Configuration	
IP Address	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. Both IPv4 and IPv6

	addresses are supported.
Receiver Configuration	
Owner	<p>Basically, sFlow can be configured in two ways: through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:</p> <ul style="list-style-type: none"> • If sFlow is currently unconfigured/unclaimed, Owner contains <none>. • If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>. • If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver. <p>If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.</p> <p>The Release 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>
IP Address/Hostname	The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.
UDP Port	The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.
Timeout	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.
Max. Datagram Size	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.
Port Configuration	
Port	The port number for which the configuration below applies.
Flow Sampler Enabled	Enables/disables flow sampling on this port.
Flow Sampler Sampling Rate	<p>The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port.</p> <p>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</p>

	back in this field.
Flow Sampler Max. Header	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 maximum datagram size does not take into account the maximum header size, samples may be dropped.
Counter Poller Enabled	Enables/disables counter polling on this port.
Counter Poller Interval	With counter polling enabled, this specifies the interval - in seconds - between counter poller samples.

Buttons	
	The Release 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). See description under Owner above.
	Click to refresh the page immediately. 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.

2.3.1.113 Redundant Ring & Chain Configuration

This page provides Redundant Ring and Redundant Chain related configuration.

Ring protection (redundancy) is used to prevent network breaks caused by link loss or network device error. Ring protection guarantees quick network reconfiguration after the loss of a network link.

Ring topologies supported include Single Ring, Dual-ring, Ring Coupling, Multiple Ring Coupling, Dual Homing, Multiple Dual Homing, Chain, and Balancing Chain. Multiple Ring types (combination of different rings) is also supported. All the ports that participate in Ring/Chain topology are configured as Trunk ports.

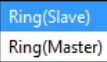
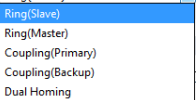
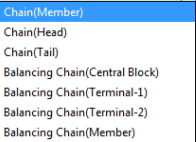
Note: when configuring a redundant ring, all switches on the same ring must be configured to use the same redundancy protocol (you can not mix Ring protocols on the same ring).

Note that Ring protection is a media redundancy protocol; you must disable any other loop protection first (before enabling the Ring/Chain):

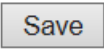
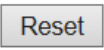
- ❑ Disable Spanning Tree at **Configuration > Spanning Tree > CIST Ports**. Click **Save**.
- ❑ Disable Loop Protection at **Configuration > Loop Protection > General Settings** and at **Configuration > Loop Protection > Port Configuration**. Click **Save** when done.

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

Object	Description
Index	<p>The group index. This parameter is used to easily identify the ring when you configuring it.</p> <p>Group 1 (Index 1) - supports configuration of Ring (slave or master).</p> <p>Group 2 (Index 2) - supports configuration of Ring, Coupling, and Dual Homing.</p> <p>Group 3 (Index 3) - supports configuration of Chain and Balancing-Chain.</p>

<p>Mode</p>	<p>Enable Ring on the specific group. When Group 1 or 2 is enabled, all configuration of Group 3 will be reset to defaults. All Group 3 configuration options will be locked.</p> <p>To configure Group 3, both Group1 and 2 must be disabled first. When Group 3 is enabled, all configuration of Group1 and 2 will be reset to defaults. All Group 1 and 2 configuration options will be locked.</p>
<p>Role</p>   	<p>Configure the Ring group on this switch as specific role.</p> <p>Group 1 - supports options of ring-master or ring-slave.</p> <p>Ring - select Ring (Master) or Ring (Slave).</p> <p>Group 2 - support configuration of the ring, coupling, and dual-homing.</p> <p>Ring - select master or slave.</p> <p>Coupling – select primary and backup.</p> <p>Dual-Homing</p> <p>Group 3 - support configuration of the chain and balancing-chain.</p> <p>Chain - select head, tail, or member.</p> <p>Balancing Chain - select 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>
<p>Ring Port(s)</p>	<p>Select ring port(s). Each ring port must be unique, CANNOT be configured in different groups; and 2 ring ports between ring/chain CANNOT be the same.</p> <ul style="list-style-type: none"> When role is ring/master, one ring port is forward port and another is block port. The block port is the redundant port; it is blocking port in normal state. When role is ring/slave, both ring ports are forward port. When role is coupling/primary, only need one ring port named primary port. When role is coupling/backup, only need one ring port named backup port. This backup port is redundant port; it is blocking port in normal state. When role is dual-homing, one ring port is primary port and another is backup port. This backup port is redundant port; it is blocking port in normal state. When role is chain/head, one ring port is member port and another is head port. Both ring ports are forwarding port in normal state. When role is chain/tail, one ring port is member port and another is tail port. The tail port is redundant port; it is blocking port in normal state. When role is chain/member, both ring ports are member port. Both ring ports are forwarding port in normal state. When role is balancing-chain/central-block, one ring port is member port and another is

	<p>block port. The block port is redundant port; it is blocking port in normal state.</p> <ul style="list-style-type: none"> When role is balancing-chain/terminal-1/2, one ring port is member port and another is terminal port. Both ring ports are forwarding port in normal state. When role is balancing-chain/member, both ring ports are member port. Both ring ports are forwarding port in normal state.
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

The table below lists the main differences between the features of the protocols. Use this information to determine which features are best suited for your network.

Feature	Ring	Ring V2	Chain	STP	RSTP
Topology	Ring	Ring	Chain	Ring, Mesh	Ring, Mesh
Recovery Time	< 300 ms	< 20 ms	< 20 ms	Up to 30 sec.	Up to 5 sec

Ringv2 Notes

- A Ring has one Master; others are slaves.
- Group 1 (Index 1) supports configuration of Ring.
- Group 2 (Index 2) supports configuration of Dual Ring, Ring Coupling, and Dual-Homing.
- Group 3 (Index 3) supports configuration of Chain and Balancing-Chain.
- All the ports that participate in a Ring/Chain topology are configured to Trunk mode. Ring Ports are configured as Trunks (at **Configuration > VLANs**).
- Do not physically connect the Ethernet cable before finishing configuring Ringv2, as this will cause a loop.
- In a VLAN environment, you must set Redundant Port, Coupling Port, and **Coupling Control** Port to join all VLANs, since these ports act as the backbone to transmit all packets of different VLANs to different switches.

Single Ring Notes

- Single Ring is the most commonly used and easily configured ring protection methods.
- With Ring Port, two ports of each device are selected as ring ports.
- Ring Roles: a Master (a forwarding port as the main path for traffic and a blocking port for the protect path, and a Slave with two forwarding ports for communication in ring).

Dual Ring Notes

- Dual ring can tolerate two links down.
- With Dual Rings, one port on each of two switches is configured as a Ring Master.

Coupling Ring Notes

- Coupling uses 2 link paths connect one Ring to another (Ring / Switch Chain, etc.).
- Coupling mode can only be enabled if the switch has already been configured Single Ring; if a switch is configured Dual Ring, this switch is prohibited having coupling).
- The 2 links configured by Coupling are redundant path for each other. Ring Port:
 - **Primary:** in the primary path of ring coupling
 - **Backup:** in the backup path of ring coupling

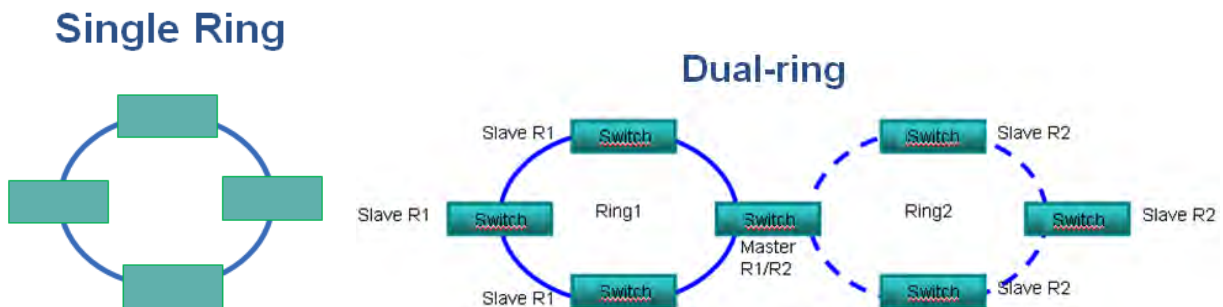
Balancing Chain Notes

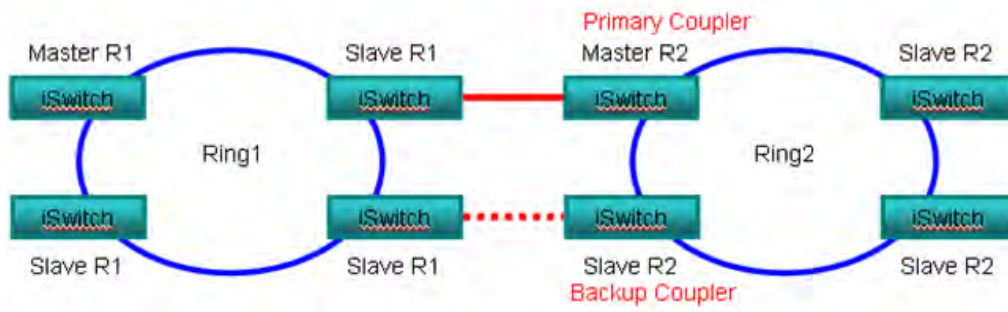
- Before configuring balancing chain, disable Ring index 1 and in index 2.
- Ring Port can include:
 - **Terminal Port:** ring ports connect between chain and another segment.
 - **Central Block Port:** a ring port in central block of balancing chain.
 - **Member Port:** the other ring port joined balancing chain topology.

Dual Homing Notes

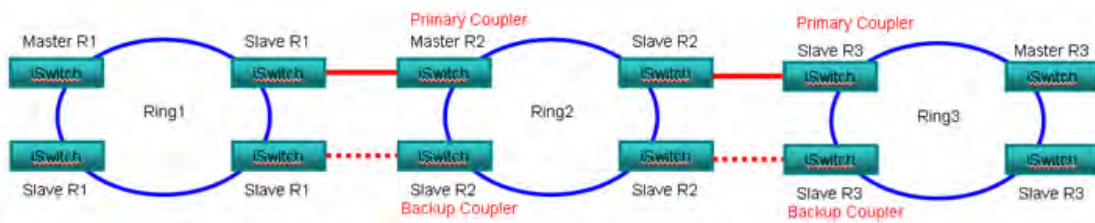
- Dual Homing uses only 1 device to connect another Ring / Switch / Chain, etc.
- Dual Homing mode can only be enabled in a switch configured as Single Ring.
- The two links run as redundant paths for each other. A Ring Port has Primary and Backup ports; both are on the same switch.

Ring Topology Examples

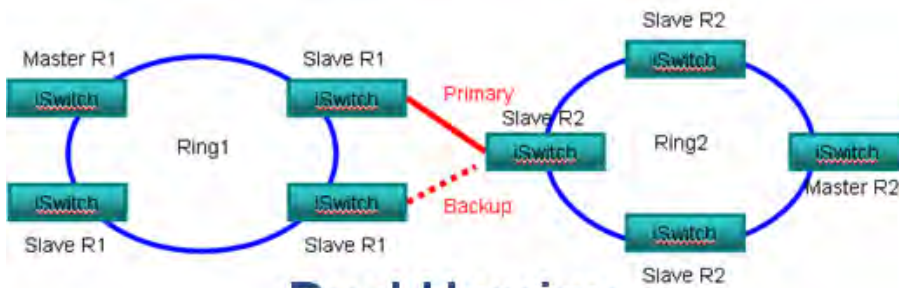




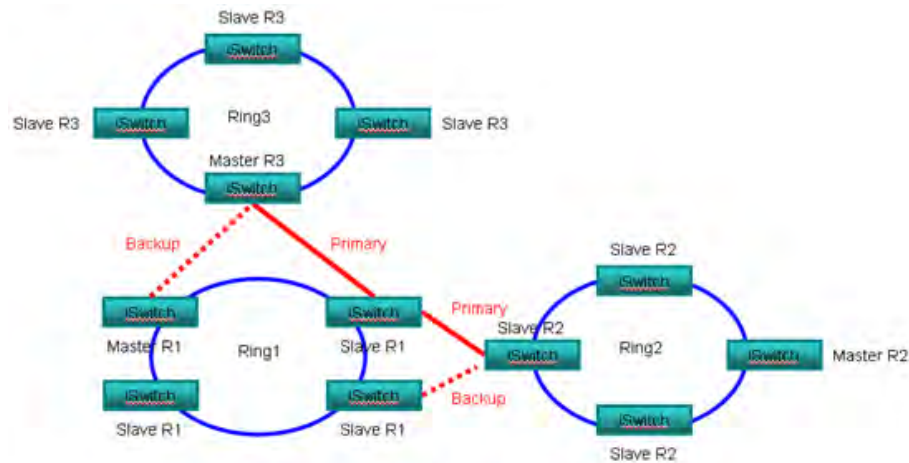
Ring Coupling



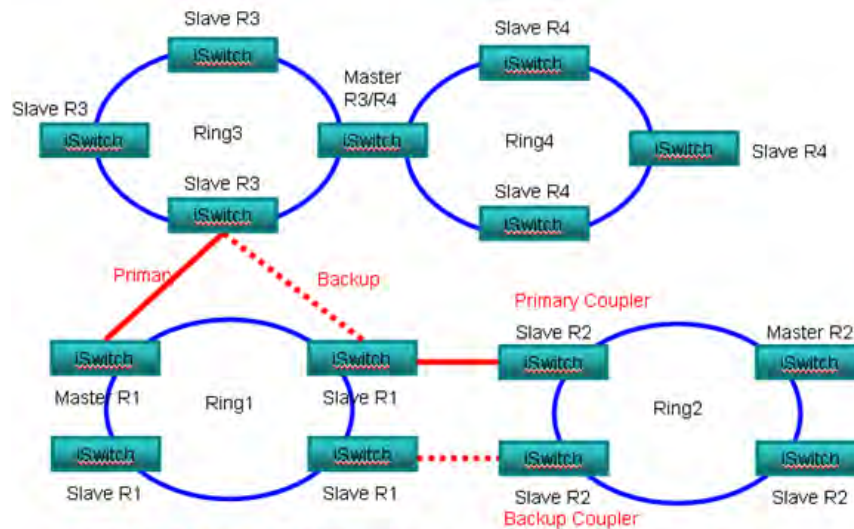
Multiple Ring Coupling



Dual Homing



Multiple Dual Homing



Multiple Ring type combination

Messages

RingV2 Configure Error Group1's two ring ports must be different.

RingV2 Configure Error Group1 and group2 must configure different ring port.

RingV2 Configure Error Group3's two chain ports must be different.

Meaning: Redundant Ring or Redundant Chain mis-configuration

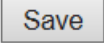
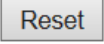
*Recovery: 1. Click the browser back button to clear the message. 2. At the "Redundant Ring and Redundant Chain Configuration" table, change one or more parameters (see above). 3. Click the **Save** button and continue.*

2.3.1.114 DDMI Configuration

This page lets you configure DDMI. Digital Diagnostics Monitoring Interface (DDMI) provides an enhanced digital diagnostic monitoring interface for optical transceivers which allows real time access to device operating parameters.



Object	Description
Mode	Indicates the DDMI mode operation. Possible modes are: Enabled: Enable DDMI mode operation. Disabled: Disable DDMI mode operation.

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

Navigate to the Monitor > DDMI menu path to view DDMI overview and details. DDMI Mode must be set to “Enabled” here in order to view DDMI overview and details.

2.4 Monitor

2.4.1.1 System

2.4.1.2 System Information

Switch system (Hardware, Time, and Software) information is provided here.

The screenshot shows the 'System Information' page for a Transition Networks switch. The page title is 'SISGM1040-184D-LRT'. The left navigation pane includes categories like Monitor, System, Information, CPU Load, IP Status, Log, Detailed Log, Alarm, Green Ethernet, Ports, DHCP, Security, LACP, Loop Protection, Spanning Tree, MVR, IPMC, and LLDP. The main content area displays the following system information:

System Information	
System	
Contact	
Name	
Location	
Hardware	
MAC Address	00-c0-f2-7a-ce-e3
Chip ID	VSC7425
Time	
System Date	2000-01-02T20:21:24+00:00
System Uptime	1d 20:21:26
Software	
Software Version	v1.00.01
Software Date	2017-02-16T21:52:37+08:00
Acknowledgments	Details

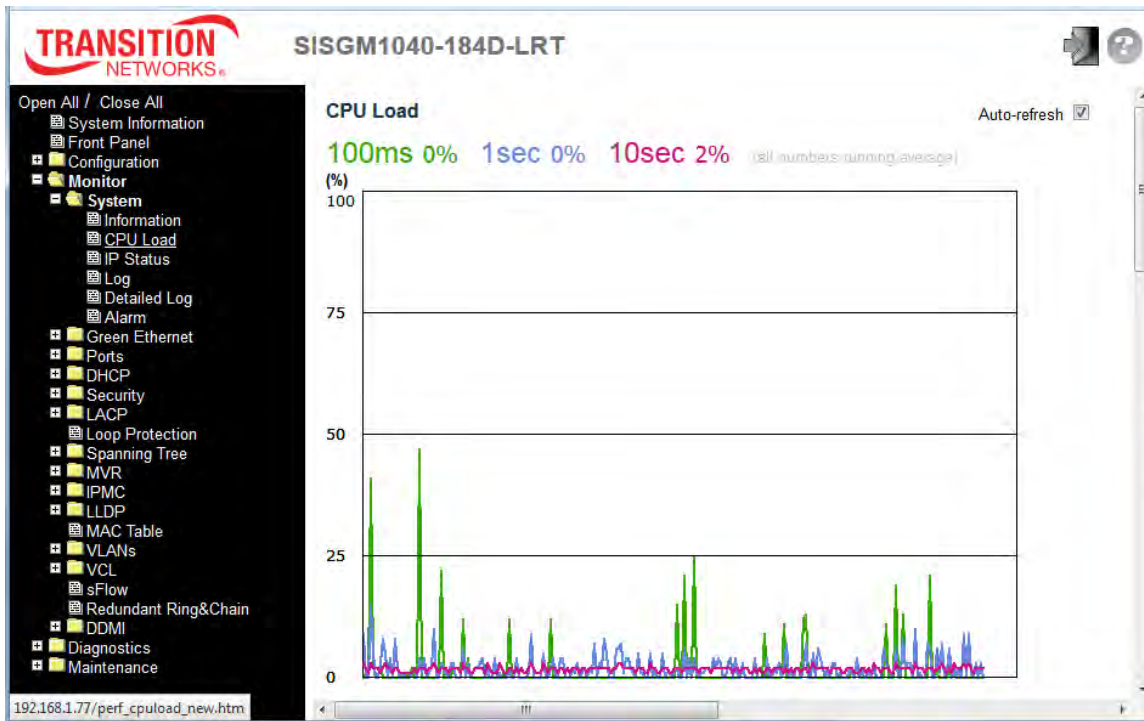
At the top right of the main content area, there are 'Auto-refresh' and 'Refresh' buttons.

Object	Description
Contact	The system contact configured at Configuration > System > Information > System Contact.
Name	The system name configured at Configuration > System > Information > System Name.
Location	The system location configured at Configuration > System > Information > System Location.
MAC Address	The MAC Address of this switch.
Chip ID	The Chip ID of this switch.
System Date	The current (GMT) system time and date. System time is obtained via the Timing server running on the switch, if any.
System Uptime	The period of time the device has been operational.
Software Version	The software version of this switch.
Software Date	The date when the switch software was produced.
Acknowledgments	Click the linked Details text to view license information.

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

2.4.1.3 CPU Load

This page displays the CPU load in a line chart. The load is measured as averaged over the last 100ms, 1sec and 10 second 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 every 3 seconds. The default is enabled (checked).

2.4.1.4 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.

TRANSITION NETWORKS SISGM1040-184D-LRT

Open All / Close All

- System Information
- Front Panel
- Configuration
- Monitor
 - System
 - Information
 - CPU Load
 - IP Status
 - Log
 - Detailed Log
 - Alarm
 - Green Ethernet
 - Ports
 - DHCP
 - Security
 - LACP
 - Loop Protection
 - Spanning Tree
 - MVR
 - IPMC
 - LLDP
 - MAC Table
 - VLANs
 - VCL
 - sFlow
 - Redundant Ring&Chain
 - DDMI

192.168.1.77/ip_status.htm

IP Interfaces Auto-refresh Refresh

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-c0-f2-7a-ce-e3	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.1.77/24	
VLAN1	IPv6	fe80:2::2c0:f2ff:fe7a:cee3/64	

IP Routes

Network	Gateway	Status
0.0.0.0/0	192.168.1.254	<UP GATEWAY HW_RT>
127.0.0.1/32	127.0.0.1	<UP HOST>
192.168.1.0/24	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
192.168.1.99	VLAN1:00-1b-11-b2-6d-4b
fe80:2::2c0:f2ff:fe7a:cee3	VLAN1:00-c0-f2-7a-ce-e3

Object	Description
IP Interfaces	
Interface	The name of the interface.
Type	The address type of the entry. This may be LINK or IPv4 or IPv6 .
Address	The current address of the interface (of the given type).
Status	The status flags of the interface (and/or address) (e.g., (e.g., UP LOOPBACK RUNNING MULTICAST).
IP Routes	
Network	The destination IP network or host address of this route.
Gateway	The gateway address of this route.
Status	The status flags of the route (e.g., UP , or UP HOST , or UP HW RT).
Neighbor cache	
IP Address	The IP address of the entry.
Link Address	The Link (MAC) address for which a binding to the IP address given exist.

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

2.4.1.5 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 **Clear** button.

The "Start from ID" input field lets you change the starting point in this table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest entry match.

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

The >> button 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.

System Log Information

Auto-refresh Refresh Clear |<< << >> >>|

Level All
Clear Level All

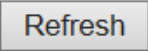
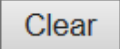



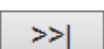
The total number of entries is 37 for the given level.

Start from ID 1 with 20 entries per page.

ID	Level	Time	Message
1	Info	1999-12-31T23:59:59+00:00	Switch just made a cool boot.
2	Info	2000-01-01T00:00:03+00:00	Link up on port 1
3	Info	2000-01-01T00:00:09+00:00	Power alarm occurs
4	Info	2000-01-01T02:08:31+00:00	Link up on port 3
5	Info	2000-01-01T02:08:31+00:00	Link up on port 4
6	Info	2000-01-01T02:08:52+00:00	Link down on port 3

Object	Description
Level	Dropdown to select the level of information to display (All , Info , Warning , or Error).
Clear Level	Dropdown to select the level of information to clear (All , Info , Warning , or Error).
ID	The linked index number of the system log entry. Click the linked ID number to display its log details.
Level	The level of the system log entry: Info : The system log entry is at information level. Warning : The system log entry is at warning level. Error : The system log entry is at error level.
Time	The time and date that the system log entry occurred.

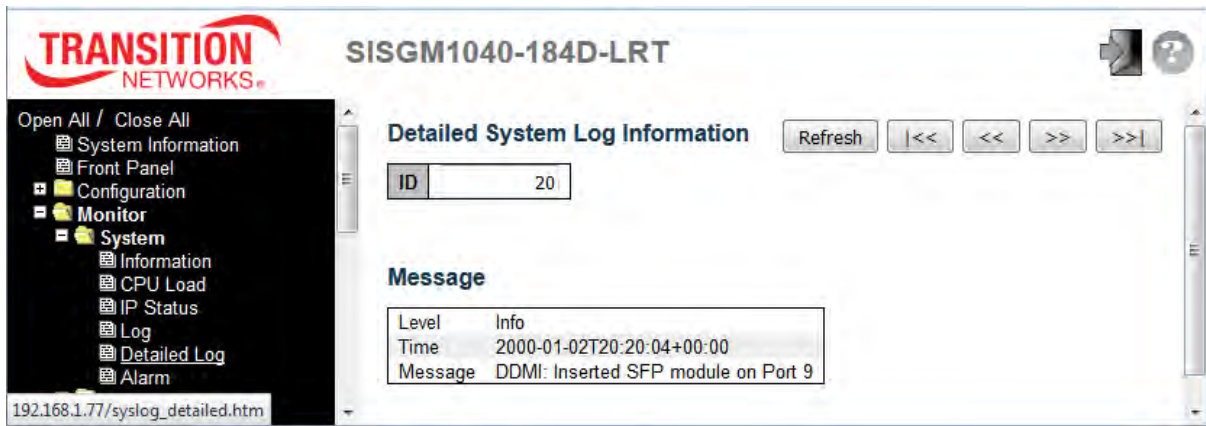
Message	The detailed message text of the system log entry (e.g., <i>Switch just made a cold boot, or Link up on Port 2.</i>
----------------	---------------------------------------------------------------------------------------------------------------------

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

2.4.1.6 Detailed System Log

The switch detailed system log information is provided here.

To display this page, navigate to the Monitor > System > Log menu path, or at the Monitor > System > Log page, click a linked ID number to display its log details.

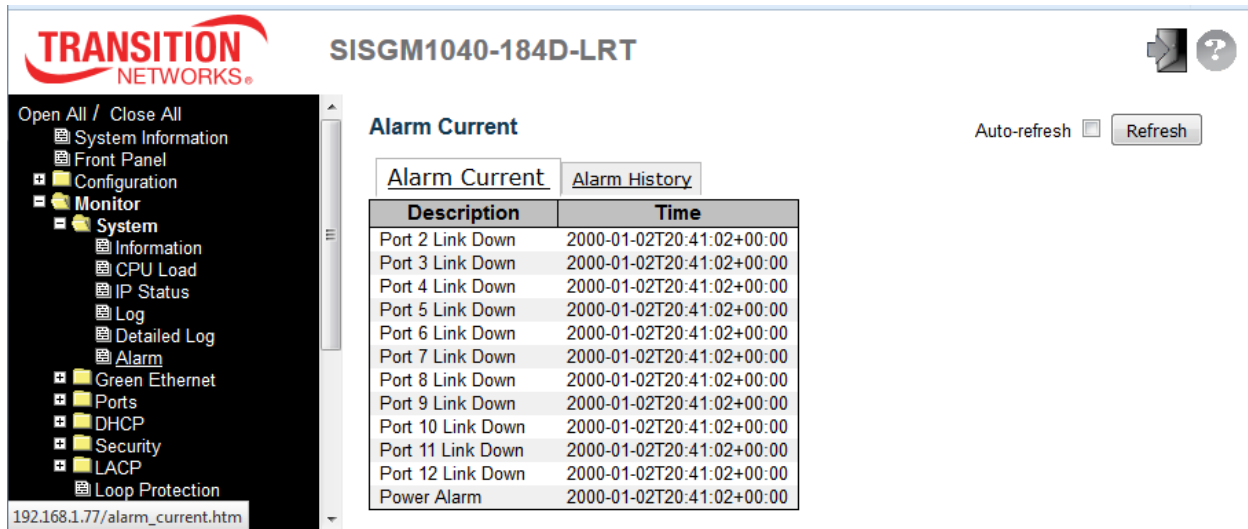


Object	Description
ID	The ID (>= 1) of the system log entry.
Message	The detailed message of the system log entry. Information includes the Level, Time, and Message text.

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.

2.4.1.7 System Alarm

Current Alarm data and an Alarm history are provided in separate tabs on this page. The Alarm Profile at Configuration > System > Alarm Profile must be enabled for alarm data to be displayed here. Otherwise the message *No entry exists* displays. The Monitor > System > Alarm > Alarm Current page is shown below:



Object	Description
Description	<p>Alarm Type Description. There are ten alarms; GE ports 1-10 generate Port Link Down. Each type can be configured to Mask and Unmask.</p> <p>The default for each type is Mask and Minor. If the alarm entry is set to Mask, then no action occurs.</p> <p>When a specified alarm condition occurs, if the alarm entry is Unmask, the switch will:</p> <ol style="list-style-type: none"> 1. Generate an entry in the current alarm table, 2. Insert one entry in the alarm history table, 3. Send an SNMP alarm trap, and 4. Trigger the alarm output relay.
Time	Alarm occurrence/cleared date and time.
State	<p>On the Alarm History tab, the Alarm State.</p> <p>Set stands for alarm occurs;</p> <p>Clear stands for alarm disappear.</p>

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

A sample Monitor > System > Alarm > Alarm History page is shown below:

TRANSITION NETWORKS SISGM1040-184D-LRT

Auto-refresh

Alarm History

Alarm Current Alarm History

Description	State	Time
Port 2 Link Down	Set	2000-01-01T20:27:53+00:00
Port 3 Link Down	Set	2000-01-01T20:27:53+00:00
Port 4 Link Down	Set	2000-01-01T20:27:53+00:00
Port 5 Link Down	Set	2000-01-01T20:27:53+00:00
Port 6 Link Down	Set	2000-01-01T20:27:53+00:00
Port 7 Link Down	Set	2000-01-01T20:27:53+00:00
Port 8 Link Down	Set	2000-01-01T20:27:53+00:00
Port 9 Link Down	Set	2000-01-01T20:27:53+00:00
Port 10 Link Down	Set	2000-01-01T20:27:53+00:00
Port 11 Link Down	Set	2000-01-01T20:27:53+00:00
Port 12 Link Down	Set	2000-01-01T20:27:53+00:00
Power Alarm	Set	2000-01-01T20:27:53+00:00
Port 2 Link Down	Clear	2000-01-01T20:30:05+00:00
Port 3 Link Down	Clear	2000-01-01T20:30:05+00:00
Port 4 Link Down	Clear	2000-01-01T20:30:05+00:00
Port 5 Link Down	Clear	2000-01-01T20:30:05+00:00
Port 6 Link Down	Clear	2000-01-01T20:30:05+00:00
Port 7 Link Down	Clear	2000-01-01T20:30:05+00:00
Port 8 Link Down	Clear	2000-01-01T20:30:05+00:00
Port 9 Link Down	Clear	2000-01-01T20:30:05+00:00
Port 10 Link Down	Clear	2000-01-01T20:30:05+00:00
Port 11 Link Down	Clear	2000-01-01T20:30:05+00:00
Port 12 Link Down	Clear	2000-01-01T20:30:05+00:00
Power Alarm	Clear	2000-01-01T20:30:05+00:00
Port 2 Link Down	Set	2000-01-01T20:36:15+00:00
Port 3 Link Down	Set	2000-01-01T20:36:15+00:00
Port 4 Link Down	Set	2000-01-01T20:36:15+00:00
Port 5 Link Down	Set	2000-01-01T20:36:15+00:00
Port 6 Link Down	Set	2000-01-01T20:36:15+00:00
Port 7 Link Down	Set	2000-01-01T20:36:15+00:00
Port 8 Link Down	Set	2000-01-01T20:36:15+00:00
Port 9 Link Down	Set	2000-01-01T20:36:15+00:00
Port 10 Link Down	Set	2000-01-01T20:36:15+00:00
Port 11 Link Down	Set	2000-01-01T20:36:15+00:00
Port 12 Link Down	Set	2000-01-01T20:36:15+00:00
Power Alarm	Set	2000-01-01T20:36:15+00:00

2.4.1.9 Green Ethernet

2.4.1.10 Port Power Savings Data

This page provides the current status for EEE (Energy Efficient Ethernet).

Port	Link	EEE	LP EEE Cap	EEE Savings	ActiPhy Savings	PerfectReach Savings
1	●	✗	✗	✗	✗	✗
2	●	✓	✗	✗	✓	✗
3	●	✓	✗	✗	✓	✗
4	●	✓	✗	✗	✓	✗
5	●	✗	✗	✗	✓	✗
6	●	✗	✗	✗	✓	✗
7	●	✓	✗	✗	✓	✗
8	●	✗	✗	✗	✓	✗
9	●	✗	✗	✗	✗	✗
10	●	✗	✗	✗	✗	✗
11	●	✗	✗	✗	✗	✗
12	●	✗	✗	✗	✗	✗

Object	Description
Port	This is the logical port number for this row.
Link	Shows if the link is up for the port (green = link up, red = link down).
EEE	Shows if EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page).
LP EEE Cap	Shows if the link partner is EEE capable.
EEE Savings	Shows if the system is currently saving power due to EEE. When EEE is enabled, the system will powered down if no frame has been received or transmitted in 5 uSec.
ActiPhy Savings	Shows if the system is currently saving power due to ActiPHY.
PerfectReach Savings	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 every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.

2.4.1.11 Ports







2.4.1.12 Ports State Overview

Each page provides an overview of the current switch port states (default).

Click the Close link to close the display.

Click the main menu Front Panel item to open the display again.


The port states are shown below:

State	Disabled	Down	Link
RJ45 ports			
SFP ports			



2.4.1.13 Traffic Overview

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


SISGM1040-184D-LRT

Open All / Close All

- System Information
- Front Panel
- Configuration
- Monitor
 - System
 - Green Ethernet
 - Ports
 - Traffic Overview
 - QoS Statistics
 - QCL Status
 - Detailed Statistics
 - DHCP
 - Security
 - LACP
 - Loop Protection
 - Spanning Tree
 - MVR

Port Statistics Overview

Auto-refresh Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered Received
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	
1	4339	4429	662587	1952775	0	0	0	0	131
2	2336	2002	1191484	211603	0	0	0	0	3
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
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
9	0	34	0	2943	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0

Object	Description
Port	The logical port for the settings contained in the same row. The Port number in each row is linked to its Detailed Port Statistics page; see Detailed Statistics below.
Packets	The number of received and transmitted packets per port.
Bytes	The number of received and transmitted bytes per port.

Errors	The number of frames received in error and the number of incomplete transmissions per port.
Drops	The number of frames discarded due to ingress or egress congestion.
Filtered	The number of received frames filtered by the forwarding process.

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

2.4.1.14 QoS Statistics

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

TRANSITION NETWORKS SISGM1040-184D-LRT

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	6401	2181	0	0	0	0	0	0	0	0	0	0	0	0	0	3524
2	2336	950	0	0	0	0	0	0	0	0	0	0	0	0	0	1052
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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
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
9	0	655	0	0	0	0	0	0	0	0	0	0	0	0	0	351
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	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.
Q0 - Q7	There are eight 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 every 3 seconds.
Refresh	Click to refresh the page immediately.
Clear	Clears the counters for all ports.

2.4.1.15 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. This page displays the configurations at the **Configuration > QoS > QoS Control List** page.

User	QCE	Port	Frame Type	Action			Conflict
				CoS	DPL	DSCP	
Static 1	1	2-12	Any	0	Default	Default	No
Static 2	2	3-10	Ethernet	1	Default	Default	No
Static 3	3	4,5,9-12	IPv4	5	Default	Default	No

Object	Description
User	Indicates the QCL user.
QCE	Indicates the QCE id.
Port	Indicates the list of ports configured with the QCE.
Frame Type	Indicates the type of frame. Possible values are: Any : Match any frame type. Ethernet : Match EtherType frames. LLC : Match (LLC) frames. SNAP : Match (SNAP) frames. IPv4 : Match IPv4 frames. IPv6 : Match IPv6 frames
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are: CoS : Classify Class of Service. DPL : Classify Drop Precedence Level. DSCP : Classify DSCP value.
Conflict	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'. Note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

Buttons	
<input type="text" value="Combined"/> ▼	Select the QCL status from this drop down list.
Auto-refresh <input checked="" type="checkbox"/>	Check this box to refresh the page automatically every 3 seconds.
<input type="button" value="Resolve Conflict"/>	Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.

2.4.1.16 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.

TRANSITION NETWORKS SISGM1040-184D-LRT

Open All / Close All
 System Information
 Front Panel
 Configuration
 Monitor
 System
 Green Ethernet
 Ports
 Traffic Overview
 QoS Statistics
 QCL Status
 Detailed Statistics
 DHCP
 Security
 LACP
 Loop Protection
 Spanning Tree
 MVR
 IPMC
 LLDP
 MAC Table
 VLANs
 VCL
 sFlow
 Redundant Ring&Chain
 DDMI
 Diagnostics
 Maintenance

Detailed Port Statistics Port 2 Port 2 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx Packets	2336	Tx Packets	2004
Rx Octets	1191484	Tx Octets	211731
Rx Unicast	949	Tx Unicast	1699
Rx Multicast	215	Tx Multicast	59
Rx Broadcast	1172	Tx Broadcast	246
Rx Pause	0	Tx Pause	2
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	1213	Tx 64 Bytes	1641
Rx 65-127 Bytes	203	Tx 65-127 Bytes	197
Rx 128-255 Bytes	91	Tx 128-255 Bytes	26
Rx 256-511 Bytes	135	Tx 256-511 Bytes	12
Rx 512-1023 Bytes	16	Tx 512-1023 Bytes	128
Rx 1024-1526 Bytes	678	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	2336	Tx Q0	950
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	1052
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	3		

http://192.168.1.77/stat_detailed.htm

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

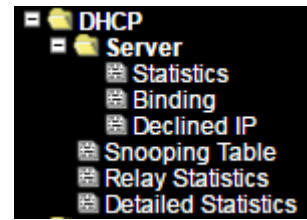
	an opcode indicating a PAUSE operation.
--	-----------------------------------------

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

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

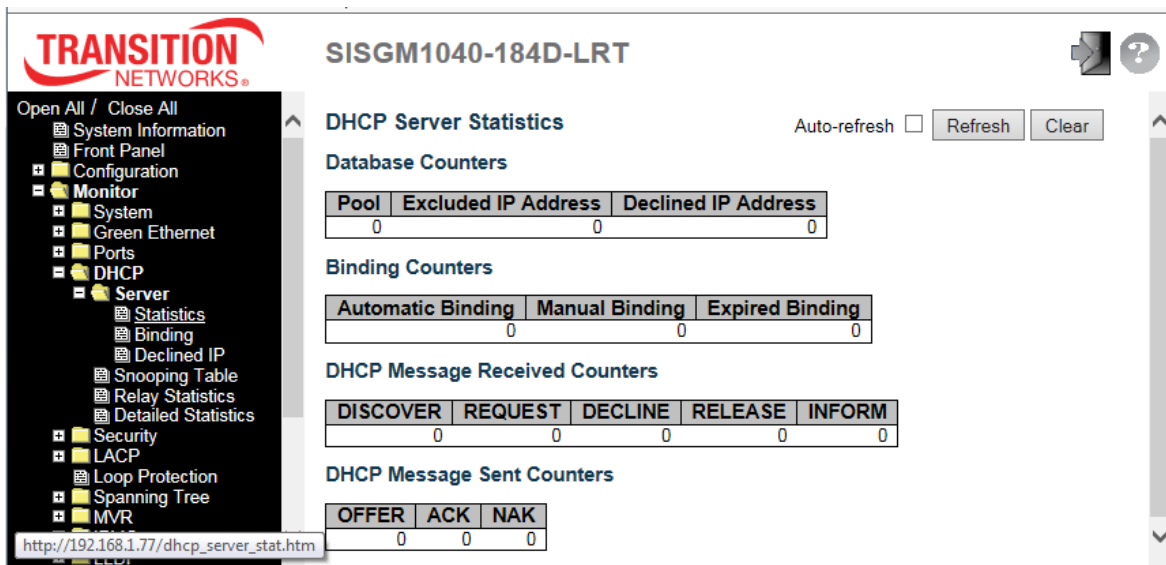
2.4.1.17 DHCP

2.4.1.18 DHCP Server



2.4.1.19 Statistics

The DHCP Server Statistics page displays the database counters and the number of DHCP messages sent and received by DHCP server.



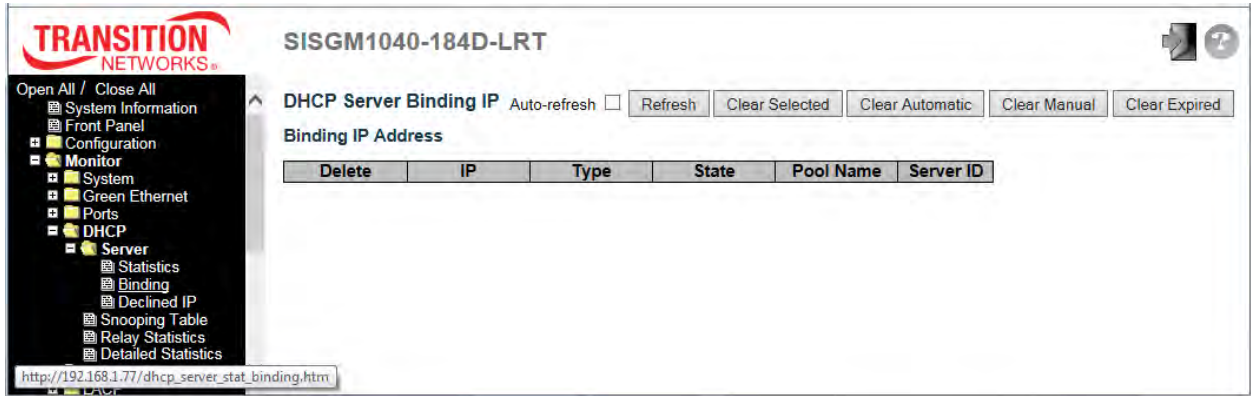
Object	Description
Database Counters	
Pool	Number of pools.
Excluded IP Address	Number of excluded IP address ranges.
Declined IP Address	Number of declined IP addresses.
Binding Counters	
Automatic Binding	Number of bindings with network-type pools.
Manual Binding	Number of bindings that administrator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

REQUEST	Number of DHCP REQUEST messages received.
DECLINE	Number of DHCP DECLINE messages received.
RELEASE	Number of DHCP RELEASE messages received.
INFORM	Number of DHCP INFORM messages received.
DHCP Message Sent Counters	
OFFER	Number of DHCP OFFER messages sent.
ACK	Number of DHCP ACK (Acknowledge) messages sent.
NAK	Number of DHCP NAK (Negative Acknowledge) messages sent.

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

2.4.1.20 Binding

This page displays bindings generated for DHCP clients.

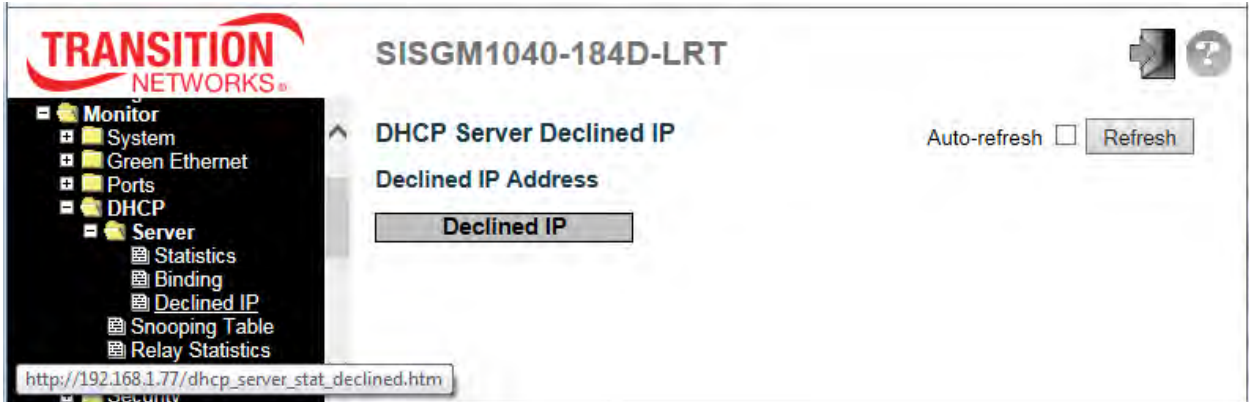


Object	Description
IP	IP address allocated to DHCP client.
Type	Type of binding. Possible types are Automatic, Manual, Expired.
State	State of binding. Possible states are Committed, Allocated, Expired.
Pool Name	The pool that generates the binding.
Server ID	Server IP address to service the binding.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.
<input type="button" value="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.
<input type="button" value="Clear Automatic"/>	Click to clear all Automatic bindings and Change them to Expired bindings.
<input type="button" value="Clear Manual"/>	Click to clear all Manual bindings and Change them to Expired bindings.
<input type="button" value="Clear Expired"/>	Click to clear all Expired bindings and free them.

2.4.1.21 Declined IP

This page displays declined IP addresses.



Object	Description
Declined IP	List of IP addresses declined by DHCP clients.

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

2.4.1.22 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 let you 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 button 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
MAC Address	User MAC address of the entry.
VLAN ID	VLAN-ID in which the DHCP traffic is permitted.
Source Port	Switch Port Number for which the entries are displayed.
IP Address	User IP address of the entry.
IP Subnet Mask	User IP subnet mask of the entry.
DHCP Server Address	DHCP Server address of the entry.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically every 3 seconds.
<input type="button" value="Refresh"/>	Refreshes the displayed table starting from the input fields.
<input type="button" value="Clear"/>	Flushes all dynamic entries.
<input type="button" value=" <<"/>	Updates the table starting from the first entry in the Dynamic DHCP snooping Table.
<input type="button" value=">>"/>	Updates the table, starting with the entry after the last entry currently displayed.

2.4.1.23 DHCP Relay Statistics

This page provides statistics for DHCP relay.

Object	Description
Server Statistics	
Transmit to Server	The number of packets that are relayed from client to server.
Transmit Error	The number of packets that resulted in errors while being sent to clients.
Receive from Server	The number of packets received from server.
Receive Missing Agent Option	The number of packets received without agent information options.
Receive Missing Circuit ID	The number of packets received with the Circuit ID option missing.
Receive Missing Remote ID	The number of packets received with the Remote ID option missing.
Receive Bad Circuit ID	The number of packets whose Circuit ID option did not match known circuit ID.
Receive Bad Remote ID	The number of packets whose Remote ID option did not match known Remote ID.
Client Statistics	
Transmit to Client	The number of relayed packets from server to client.
Transmit Error	The number of packets that resulted in error while being sent to servers.
Receive from Client	The number of received packets from server.
Receive Agent Option	The number of received packets with relay agent information option.
Replace Agent Option	The number of packets which were replaced with relay agent information option.
Keep Agent Option	The number of packets whose relay agent information was retained.
Drop Agent Option	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 every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.
<input type="button" value="Clear"/>	Clear all statistics.

2.4.1.24 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. Clearing the statistics on a specific port may not take effect on global statistics since it gathers the different layer overview.

The screenshot shows the 'DHCP Detailed Statistics Port 1' page. The table below represents the data shown in the screenshot:

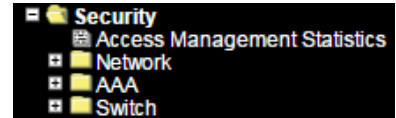
Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
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
Rx and Tx Discover	The number of discover (option 53 with value 1) packets received and transmitted.
Rx and Tx Offer	The number of offer (option 53 with value 2) packets received and transmitted.
Rx and Tx Request	The number of request (option 53 with value 3) packets received and transmitted.
Rx and Tx Decline	The number of decline (option 53 with value 4) packets received and transmitted.
Rx and Tx ACK	The number of ACK (option 53 with value 5) packets received and transmitted.
Rx and Tx NAK	The number of NAK (option 53 with value 6) packets received and transmitted.
Rx and Tx Release	The number of release (option 53 with value 7) packets received and transmitted.
Rx and Tx Inform	The number of inform (option 53 with value 8) packets received and transmitted.
Rx and Tx Lease Query	The number of lease query (option 53 with value 10) packets received and transmitted.
Rx and Tx Lease Unassigned	The number of lease unassigned (option 53 with value 11) packets received and transmitted.
Rx and Tx Unknown	The number of lease unknown (option 53 with value 12) packets received and transmitted.
Rx and Tx Active	The number of lease active (option 53 with value 13) packets received and transmitted.

Rx Discarded checksum error	The number of discard packet that IP/UDP checksum is error.
Rx Discarded from Untrusted	The number of discarded packet that are coming from untrusted port.

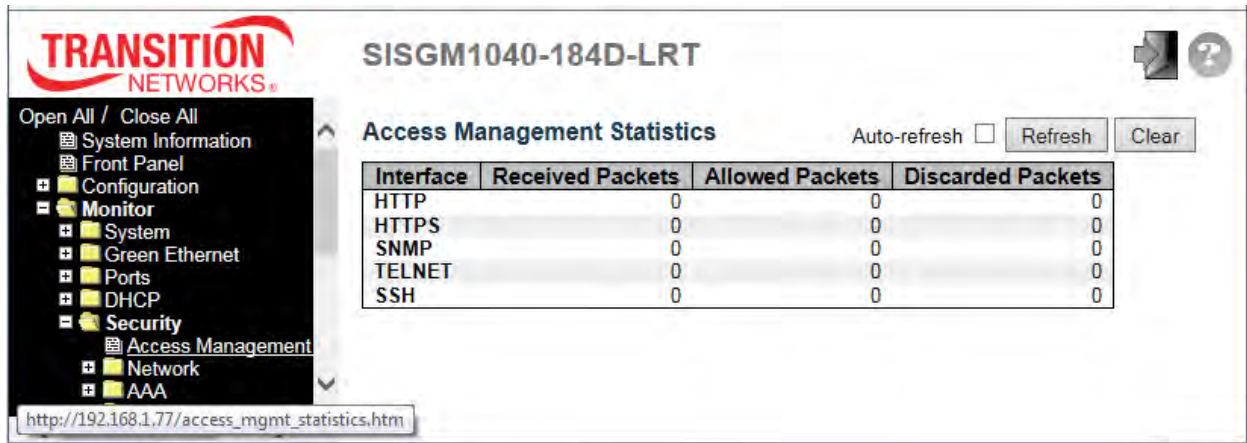
Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically every 3 seconds.
<input type="button" value="Refresh"/>	Refreshes the displayed table starting from the input fields.
<input type="button" value="Clear"/>	Flushes all dynamic entries.

2.4.1.25 Security



2.4.1.26 Access Management Statistics

This page provides statistics for access management.



Object	Description
Interface	The interface type through which the remote host can access the switch.
Received Packets	Number of received packets from the interface when access management mode is enabled.
Allowed Packets	Number of allowed packets from the interface when access management mode is enabled.
Discarded Packets	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 every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.
<input type="button" value="Clear"/>	Clear all statistics.

2.4.1.27 Network

2.4.1.28 Port Security

2.4.1.29 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.

The screenshot shows the web interface for 'SISGM1040-184D-LRT'. The left sidebar contains a navigation tree with 'Port Security' expanded. The main content area is titled 'Port Security Switch Status' and includes an 'Auto-refresh' checkbox and a 'Refresh' button. Below this is the 'User Module Legend' table:

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

Below the legend is the 'Port Status' table:

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

Object	Description
User Module Legend	
User Module Name	The full name of a module that may request Port Security services. Each of the user modules has a column that shows whether that module has enabled

	<p>Port Security.</p> <p>A dash (-) means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr below) has enabled port security.</p>
Abbr	<p>A one-letter abbreviation of the user module. This is used in the Users column in the port status table. Limit Control = L, 802.1X = 8, DHCP Snooping = D and Voice VLAN = V.</p>

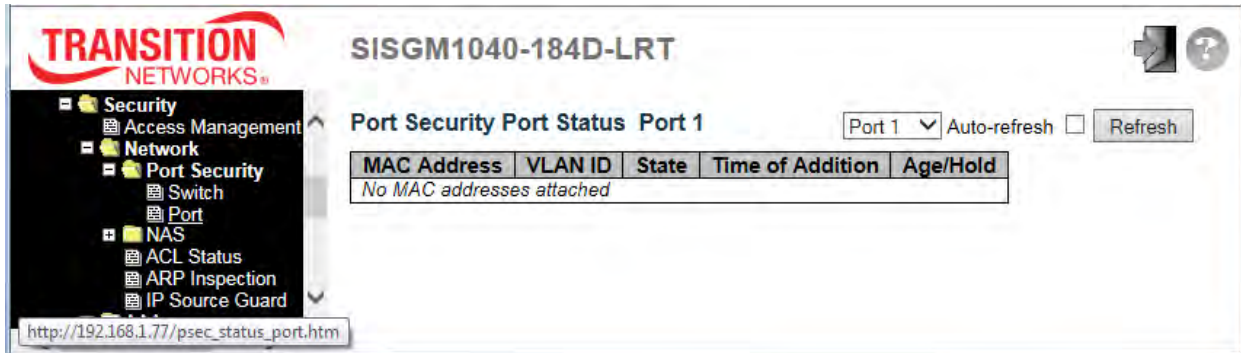
Port Status	
Port	<p>The port number for which the status applies. Click the port number to see the status for this particular port.</p>
Users	<p>Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.</p>
State	<p>Shows the current state of the port. It can take one of four values:</p> <p>Disabled: No user modules are currently using the Port Security service.</p> <p>Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.</p> <p>Limit Reached: 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.</p> <p>Shutdown: 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.</p>
MAC Count (Current, Limit)	<p>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.</p> <p>If no user modules are enabled on the port, the Current column will show a dash (-).</p> <p>If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).</p>

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

2.4.1.30 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
MAC Address & VLAN ID	The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.
State	Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.
Time of Addition	Shows the date and time when this MAC address was first seen on the port.
Age/Hold	<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 (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.</p> <p>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 every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.

2.4.1.31 NAS

2.4.1.32 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	Authorized			-	
2	Force Authorized	Link Down			-	
3	Force Authorized	Link Down			-	
4	Force Authorized	Link Down			-	
5	Force Unauthorized	Link Down			-	
6	Port-based 802.1X	Link Down			-	
7	Single 802.1X	Link Down			-	
8	Multi 802.1X	Link Down			-	
9	MAC-based Auth.	Link Down			-	
10	Force Authorized	Link Down			-	
11	Force Authorized	Link Down			-	
12	Force Authorized	Link Down			-	

Object	Description
Port	The switch port number. Click to navigate to detailed NAS statistics for this port.
Admin State	The port's current administrative state. See "NAS Admin State" on page 69 for valid values.
Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.
Last Source	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.
Last ID	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.
QoS Class	QoS Class assigned to the port by the RADIUS server if enabled.
Port VLAN ID	The VLAN ID that NAS has put the port in. The field is blank if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

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

2.4.1.33 Port

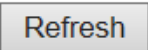
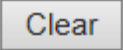
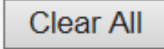
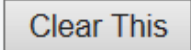
This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics only. Use the port select box to select which port details to be displayed.



Object	Description
Port State	
Admin State	The port's current administrative state. See NAS Admin State on page 69 for a description of possible values.
Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.
QoS Class	The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.
Port VLAN ID	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.
Port Counters	
EAPOL Counters	These supplicant frame counters are available for the following administrative states: <ul style="list-style-type: none"> • Force Authorized • Force Unauthorized • Port-based 802.1X • Single 802.1X • Multi 802.1X

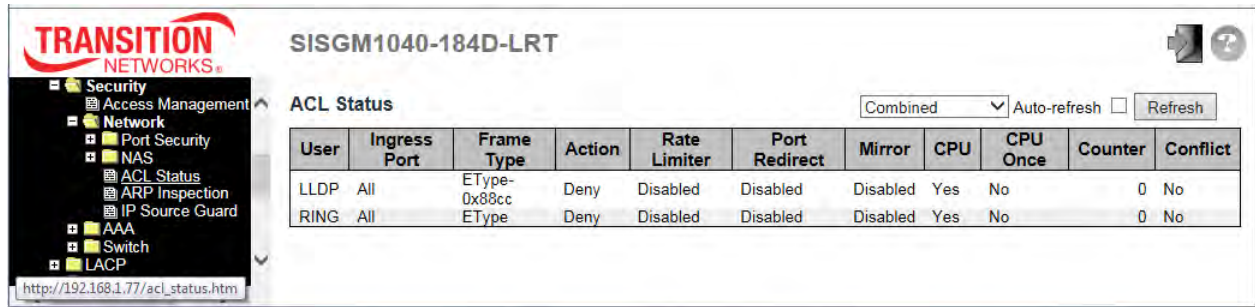
Backend Server Counters	<p>These backend (RADIUS) frame counters are available for the following administrative states:</p> <ul style="list-style-type: none"> • Port-based 802.1X • Single 802.1X • Multi 802.1X • MAC-based Auth.
Last Supplicant/Client Info	<p>Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:</p> <ul style="list-style-type: none"> • Port-based 802.1X • Single 802.1X • Multi 802.1X • MAC-based Auth.
Selected Counters	
Selected Counters	<p>The Selected Counters table is visible when the port is in one of the following administrative states:</p> <ul style="list-style-type: none"> • Multi 802.1X • MAC-based Auth. <p>The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.</p>
Attached MAC Addresses	
Identity	<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>
MAC Address	<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>
VLAN ID	<p>This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.</p>
State	<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</p>

	blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.
Last Authentication	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 every 3 seconds.
	Click to refresh the page immediately.
	<p>This button is available in these modes:</p> <ul style="list-style-type: none"> • Force Authorized • Force Unauthorized • Port-based 802.1X • Single 802.1X <p>Click to clear the counters for the selected port.</p>
	<p>This button is available in these modes:</p> <ul style="list-style-type: none"> • Multi 802.1X • MAC-based Auth.X <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 these modes:</p> <ul style="list-style-type: none"> • Multi 802.1X • MAC-based Auth.X <p>Click to clear only the currently selected client's counters.</p>

2.4.1.34 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.



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

Port Redirect	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.
Mirror	Specify the mirror operation of this port. The allowed values are: Enabled : Frames received on the port are mirrored. Disabled : Frames received on the port are not mirrored. The default value is "Disabled".
CPU	Forward packet that matched the specific ACE to CPU.
CPU Once	Forward first packet that matched the specific ACE to CPU.
Counter	The counter indicates the number of times the ACE was hit by a frame.
Conflict	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 every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.
<div style="border: 1px solid black; padding: 2px;"> Combined ▼ Combined Static IP Source Guard IPMC ARP Inspection DHCP Loop Protect RING LLDP Conflict </div>	User dropdown; lets you specify the set of user status to be displayed (Combined, Static, IP Source Guard, IPMC, ARP Inspection, DHCP, Loop Protect, RING, LLDP, Conflict).

2.4.1.35 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 lets you 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 button 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
Port	Switch Port Number for which the entries are displayed.
VLAN ID	VLAN ID (VID) in which the ARP traffic is permitted.
MAC Address	User MAC address of the entry.
IP Address	User IP address of the entry.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically every 3 seconds.
<input type="button" value="Refresh"/>	Refreshes the displayed table starting from the input fields.
<input type="button" value="Clear"/>	Flushes all dynamic entries.
<input type="button" value=" <<"/>	Updates the table starting from the first entry in the Dynamic ARP Inspection Table.
<input type="button" value=">>"/>	Updates the table, starting with the entry after the last entry currently displayed.

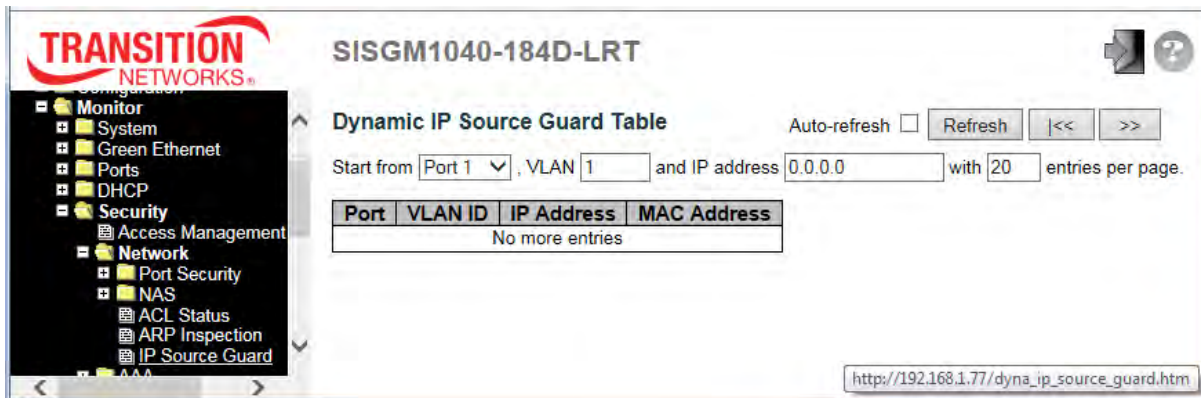
2.4.1.36 IP Source Guard

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 let you select the starting point in the Dynamic IP Source Guard Table. Clicking the **Refresh** 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 **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> button 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" displays in the table. Use the |<< button to start over.



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

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

2.4.1.37 AAA

2.4.1.38 RADIUS Overview

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

TRANSITION NETWORKS SISGM1040-184D-LRT

RADIUS Authentication Server Status Overview

#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

Auto-refresh Refresh

http://192.168.1.77/auth_status_radius_overview.htm

Object	Description
RADIUS Authentication Servers	
#	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
Status	The current status of the server. This field takes one of the following values: Disabled: The server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): 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.
RADIUS Accounting Servers	
#	The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
Status	<p>The current status of the server. This field takes one of the following values:</p> <p>Disabled: The server is disabled.</p> <p>Not Ready: The server is enabled, but IP communication is not yet up and running.</p> <p>Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.</p> <p>Dead (X seconds left): 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 every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.

2.4.1.39 RADIUS Details

This page provides detailed statistics for a particular RADIUS server.

The screenshot shows the 'RADIUS Details' page for 'Server #1'. It features a left-hand navigation tree with categories like System Information, Configuration, Monitor, System, Green Ethernet, Ports, DHCP, Security, Access Management, Network, AAA, Switch, LACP, Loop Protection, Spanning Tree, MVR, IPMC, LLDP, MAC Table, VLANs, VCL, sFlow, Redundant Ring&Chain, DDMI, and Diagnostics. The main content area displays two tables: 'RADIUS Authentication Statistics for Server #1' and 'RADIUS Accounting Statistics for Server #1'. Each table has columns for 'Receive Packets' and 'Transmit Packets', with sub-headers for various metrics. Below each table is an 'Other Info' section with fields for IP Address, State, and Round-Trip Time. Control buttons for 'Auto-refresh', 'Refresh', and 'Clear' are visible at the top right of the statistics area.

RADIUS Authentication Statistics for Server #1	
Receive Packets	Transmit Packets
Access Accepts	Access Requests
Access Rejects	Access Retransmissions
Access Challenges	Pending Requests
Malformed Access Responses	Timeouts
Bad Authenticators	
Unknown Types	
Packets Dropped	
Other Info	
IP Address	0.0.0.0
State	Disabled
Round-Trip Time	0 ms

RADIUS Accounting Statistics for Server #1	
Receive Packets	Transmit Packets
Responses	Requests
Malformed Responses	Retransmissions
Bad Authenticators	Pending Requests
Unknown Types	Timeouts
Packets Dropped	
Other Info	
IP Address	0.0.0.0
State	Disabled
Round-Trip Time	0 ms

Object	Description
RADIUS Authentication Statistics	
Packet Counters	RADIUS authentication server packet counter. There are seven receive and four transmit counters.
Other Info	This section contains information about the state of the server and the latest round-trip time.
RADIUS Accounting Statistics	
Packet Counters	RADIUS accounting server packet counter. There are five receive and four transmit counters.
Other Info	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 every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.
<input type="button" value="Clear"/>	Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

2.4.1.40 Switch


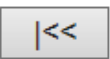
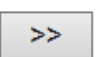
2.4.1.41 RMON

2.4.1.42 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
ID	Indicates the index of Statistics entry.
Data Source(ifIndex)	The port ID which wants to be monitored.
Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
Octets	The total number of octets of data (including those in bad packets) received on the network.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broad-cast	The total number of good packets received that were directed to the broadcast address.
Multi-cast	The total number of good packets received that were directed to a multicast address.
CRC Errors	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).
Under-Size	The total number of packets received that were less than 64 octets.
Over-size	The total number of packets received that were longer than 1518 octets.

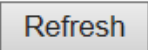
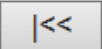

Frag.	The number of frames which size is less than 64 octets received with invalid CRC.
Jabb.	The number of frames which size is larger than 64 octets received with invalid CRC.
Coll.	The best estimate of the total number of collisions on this Ethernet segment.
64	The total number of packets (including bad packets) received that were 64 octets in length.
65~127	The total number of packets (including bad packets) received that were from 65 to 127 octets in length.
128~255	The total number of packets (including bad packets) received that were from 128 to 255 octets in length.
256~511	The total number of packets (including bad packets) received that were from 256 to 511 octets in length.
512~1023	The total number of packets (including bad packets) received that were from 512 to 1023 octets in length.
1024~1588	The total number of packets (including bad packets) received that were from 1024 to 1588 octets in length.

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

2.4.1.43 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
History Index	Indicates the index of History control entry.
Sample Index	Indicates the index of the data entry associated with the control entry.
Sample Start	The value of sysUpTime at the start of the interval over which this sample was measured.
Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
Octets	The total number of octets of data (including those in bad packets) received on the network.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broadcast	The total number of good packets received that were directed to the broadcast address.
Multicast	The total number of good packets received that were directed to a multicast address.
CRC Errors	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).
Undersize	The total number of packets received that were less than 64 octets.
Oversize	The total number of packets received that were longer than 1518 octets.
Frag.	The number of frames which size is less than 64 octets received with invalid CRC.
Jabb.	The number of frames which size is larger than 64 octets received with invalid CRC.
Coll.	The best estimate of the total number of collisions on this Ethernet segment.
Utilization	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 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.


2.4.1.44 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.

The screenshot shows the web interface for SISGM1040-184D-LRT. On the left is a navigation tree with categories like Monitor, System, Green Ethernet, Ports, DHCP, Security, Network, AAA, Switch, and RMON. The RMON section is expanded to show Statistics, History, Alarm, and Event. The main content area is titled 'RMON Alarm Overview' and includes an 'Auto-refresh' checkbox, a 'Refresh' button, and navigation arrows. Below this is a text field for 'Start from Control Index' (set to 0) and 'entries per page' (set to 20). A table with 10 columns is shown, but it contains the text 'No more entries'.

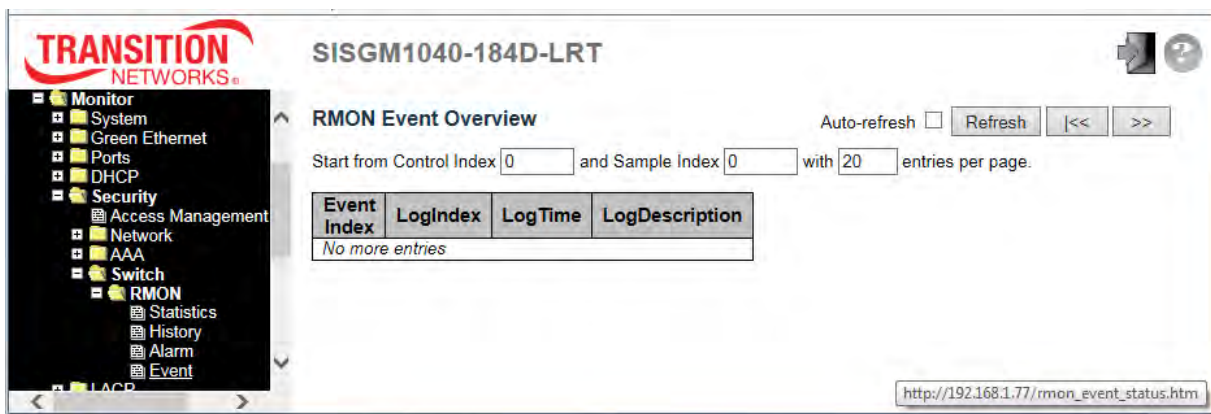
Object	Description
ID	Indicates the index of Alarm control entry.
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold.
Variable	Indicates the particular variable to be sampled.
Sample Type	The method of sampling the selected variable and calculating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

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.
<input type="button" value=" <<"/>	Updates the table starting from the first entry, i.e. the entry with the lowest ID.

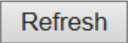


	Updates the table, starting with the entry after the last entry currently displayed.
-----------------------------------------------------------------------------------	--------------------------------------------------------------------------------------

2.4.1.45 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
Event Index	Indicates the index of the event entry.
Log Index	Indicates the index of the log entry.
Log Time	Indicates the time and date of the Event.
LogDescription	Indicates the Event description.

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

2.4.1.46 LACP

2.4.1.47 System Status

This page provides a status overview for all LACP instances.

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


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

2.4.1.48 Port Status

This page provides a status overview for LACP status for all ports.

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	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-
11	No	-	-	-	-	-
12	No	-	-	-	-	-

Object	Description
Port	The switch port number.
LACP	'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.
Key	The key assigned to this port. Only ports with the same key can aggregate together.
Aggr ID	The Aggregation ID assigned to this aggregation group.
Partner System ID	The partner's System ID (MAC address).
Partner Port	The partner's port number connected to this port.
Partner Prio	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 every 3 seconds.

2.4.1.49 Port Statistics

This page provides an overview for LACP statistics for all ports.

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	73	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
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0

Object	Description
Port	The switch port number.
LACP Received	Shows how many LACP frames have been received at each port.
LACP Transmitted	Shows how many LACP frames have been sent from each port.
Discarded	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 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.

2.4.1.50 Loop Protection

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

The screenshot shows the web interface for a Transition Networks switch. On the left is a navigation tree with categories like Monitor, System, Green Ethernet, Ports, DHCP, Security, LACP, Loop Protection, Spanning Tree, MVR, IPMC, LLDP, MAC Table, VLANs, VCL, and sFlow. The main content area is titled 'SISGM1040-184D-LRT' and 'Loop Protection Status'. It features an 'Auto-refresh' checkbox and a 'Refresh' button. Below these is a table with the following data:

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Log Only	Enabled	0	Up	-	-
2	Log Only	Enabled	0	Down	-	-
3	Shutdown+Log	Disabled	0	Down	-	-
4	Shutdown	Disabled	0	Down	-	-
5	Shutdown+Log	Enabled	0	Down	-	-
6	Shutdown+Log	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-
9	Shutdown	Enabled	0	Up	-	-
10	Shutdown	Enabled	0	Down	-	-

Object	Description
Port	The switch port number of the logical port.
Action	The currently configured port action (<i>Log Only</i> , or <i>Shutdown + Log</i> or <i>Shutdown</i>).
Transmit	The currently configured port transmit mode (<i>Enabled</i> or <i>Disabled</i>).
Loops	The number of loops detected on this port.
Status	The current loop protection status of the port (<i>Up</i> or <i>Down</i>).
Loop	Whether a loop is currently detected on the port.
Time of Last Loop	The time of the last loop event detected.

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

2.4.1.51 Spanning Tree

2.4.1.52 Bridge Status

This page provides a status overview of all STP bridge instances.

The screenshot shows the 'STP Bridges' page in the Transition Networks web interface. The page title is 'SISGM1040-184D-LRT'. On the left is a navigation tree with 'Spanning Tree' expanded to 'Bridge Status'. The main content area shows a table of STP Bridges with columns for MSTI, Bridge ID, Root ID, Port, Cost, Topology Flag, and Topology Change Last. There are also 'Auto-refresh' and 'Refresh' buttons.

MSTI	Bridge ID	Root		Topology Flag	Topology Change Last
		ID	Port Cost		
CIST	32768.00-C0-F2-7A-CE-E3	32768.00-C0-F2-7A-CE-E3	- 0	Steady	-
MSTI1	32769.00-C0-F2-7A-CE-E3	32769.00-C0-F2-7A-CE-E3	- 0	Steady	-
MSTI2	32770.00-C0-F2-7A-CE-E3	32770.00-C0-F2-7A-CE-E3	- 0	Steady	-
MSTI3	32771.00-C0-F2-7A-CE-E3	32771.00-C0-F2-7A-CE-E3	- 0	Steady	-

Object	Description
MSTI	The Bridge Instance. This is also a link to the STP Detailed Bridge Status (shown on the next page).
Bridge ID	The Bridge ID of this Bridge instance.
Root ID	The Bridge ID of the currently elected root bridge.
Root Port	The switch port currently assigned the <i>root</i> port role.
Root Cost	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.
Topology Flag	The current state of the Topology Change Flag of this Bridge instance.
Topology Change Last	The time since last Topology Change occurred.

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

STP Detailed Bridge Status Example

Click on a linked MSTI instance to display this page (see “Bridge Status” above).

TRANSITION NETWORKS SISGM1040-184D-LRT

Open All / Close All

- System Information
- Front Panel
- Configuration
- Monitor
 - System
 - Green Ethernet
 - Ports
 - DHCP
 - Security
 - LACP
 - Loop Protection
 - Spanning Tree
 - Bridge Status
 - Port Status
 - Port Statistics
 - MVR
 - IPMC
 - LLDP
 - MAC Table
 - VLANs
 - VCL

STP Detailed Bridge Status Auto-refresh Refresh

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	28672.00-C0-F2-7A-CE-E3
Root ID	28672.00-C0-F2-7A-CE-E3
Root Cost	0
Root Port	-
Regional Root	28672.00-C0-F2-7A-CE-E3
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	9
Topology Change Last	0d 02:13:52

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
1	128:001	DesignatedPort	Forwarding	24	Yes	Yes	0d 00:06:12
9	128:009	DesignatedPort	Forwarding	200000	Yes	Yes	0d 00:06:12

2.4.1.53 Port Status

This page displays the STP CIST port status for physical ports of the switch.

The screenshot shows the web interface for a Transition Networks switch. The main content area displays the 'STP Port Status' for device 'SISGM1040-184D-LRT'. A table lists 12 ports with their CIST Role, CIST State, and Uptime. Ports 1 and 9 are in a 'Forwarding' state, while all other ports are in a 'Discarding' state. The interface also features an 'Auto-refresh' checkbox (unchecked) and a 'Refresh' button.

Port	CIST Role	CIST State	Uptime
1	DesignatedPort	Forwarding	0d 00:07:58
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	DesignatedPort	Forwarding	0d 00:07:58
10	Disabled	Discarding	-
11	Disabled	Discarding	-
12	Disabled	Discarding	-

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

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

2.4.1.54 Port Statistics

This page displays the STP port statistics counters of bridge ports in the switch.

The screenshot shows the 'STP Statistics' page for switch SISGM1040-184D-LRT. The page features a navigation menu on the left with categories like Monitor, System, Green Ethernet, Ports, DHCP, Security, LACP, Loop Protection, Spanning Tree, Bridge Status, Port Status, Port Statistics, and MVR. The main content area displays a table of STP statistics for two ports (1 and 9). The table has columns for Transmitted (MSTP, RSTP, STP, TCN), Received (MSTP, RSTP, STP, TCN), and Discarded (Unknown, Illegal). Below the table are buttons for 'Auto-refresh' (checkbox), 'Refresh', and 'Clear'. A URL bar at the bottom right shows 'http://192.168.1.77/mstp_statistics.htm'.

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	3829	287	0	0	0	0	0	0	0	0
9	3174	287	0	0	0	0	0	0	0	0

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

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

2.4.1.55 MVR

2.4.1.56 MVR Statistics

This page provides MVR Statistics information.

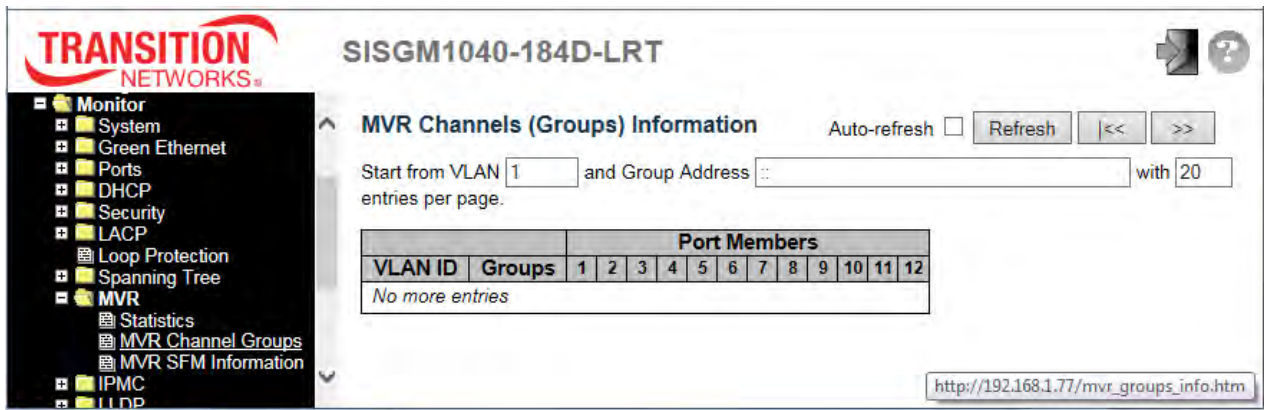
VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
10	0 / 0	0 / 0	0	0 / 0	0 / 0	0 / 0
20	0 / 0	0 / 0	0	0 / 0	0 / 0	0 / 0

Object	Description
VLAN ID	The Multicast VLAN ID.
IGMP/MLD Queries Received	The number of Received Queries for IGMP and MLD, respectively.
IGMP/MLD Queries Transmitted	The number of Transmitted Queries for IGMP and MLD, respectively.
IGMPv1 Joins Received	The number of Received IGMPv1 Joins.
IGMPv2/MLDv1 Reports Received	The number of Received IGMPv2 Joins and MLDv1 Reports, respectively.
IGMPv3/MLDv2 Reports Received	The number of Received IGMPv1 Joins and MLDv2 Reports, respectively.
IGMPv2/MLDv1 Leaves Received	The number of Received IGMPv2 Leaves and MLDv1 Dones, respectively.

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

2.4.1.57 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 lets you select the starting point in the MVR Channels (Groups) Information Table. Click the **Refresh** button to 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 **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The >> button 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" displays in the table. Use the |<< button to start over.



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

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically every 3 seconds.
<input type="button" value="Refresh"/>	Refreshes the displayed table starting from the input fields.
<input type="button" value=" <<"/>	Updates the table starting from the first entry in the MVR Channels (Groups) Information table.
<input type="button" value=">>"/>	Updates the table, starting with the entry after the last entry currently displayed.

2.4.1.58 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 lets you select the starting point in the MVR SFM Information Table. Click the **Refresh** button to 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 **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The >> button 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
VLAN ID	VLAN ID of the group.
Group	Group address of the group displayed.
Port	Switch port number.
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
Source Address	IP 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.
Type	Indicates the Type. It can be either Allow or Deny.
Hardware Filter/Switch	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 every 3 seconds.
<input type="button" value="Refresh"/>	Refreshes the displayed table starting from the input fields.
<input type="button" value=" <<"/>	Updates the table starting from the first entry in the MVR SFM Information Table.
<input type="button" value=">>"/>	Updates the table, starting with the entry after the last entry currently displayed.

2.4.1.59 IPMC

2.4.1.60 IGMP Snooping

2.4.1.61 IGMP Snooping Status

This page provides IGMP Snooping status.

The screenshot displays the IGMP Snooping Status page. The main content area features a table with the following data:

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
10	v3	v3	ACTIVE	0	0	0	0	0	0
20	v1	v1	ACTIVE	0	0	0	0	0	0
40	v3	v3	IDLE	0	0	0	0	0	0

Below the statistics table is a 'Router Port' table:

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-

Object	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	Working Querier Version currently.
Host Version	Working Host Version currently.
Querier Status	Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.
Querier Transmitted	The number of Transmitted Queries.
Queries Received	The number of Received Queries.
V1 Report Received	The number of Received V1 Reports.
V2 Report Received	The number of Received V2 Reports.
V3 Report Received	The number of Received V3 Reports.
V2 Leaves Received	The number of Received V2 Leaves.
Router Port	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 IGMP querier.

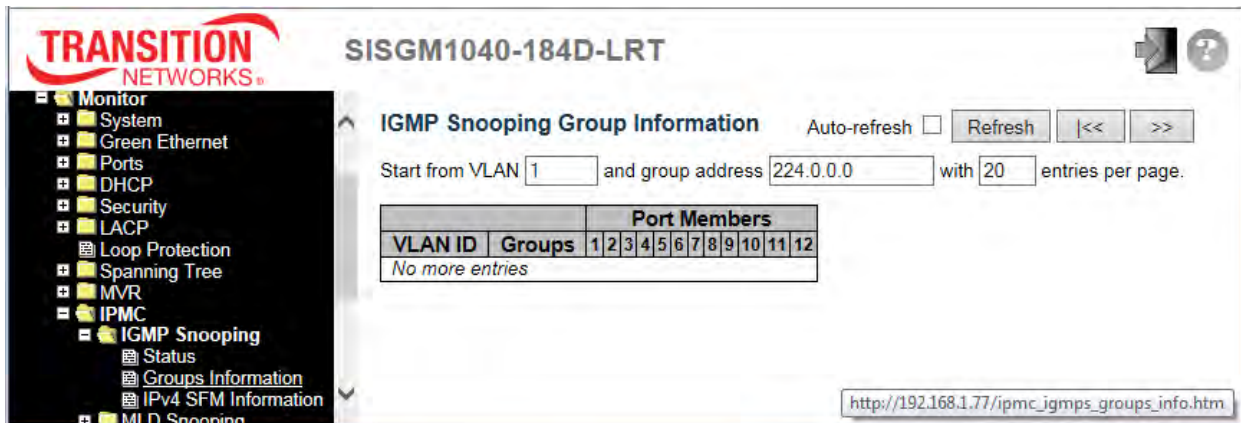
	Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.
Port	Switch port number.
Status	Indicate whether specific port is a router port or not.

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

2.4.1.62 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 lets you select the starting point in the IGMP Group Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next IGMP Group Table match. Also, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The >> button 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
VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port Members	Ports under this group.

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

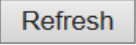
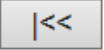

2.4.1.63 IPv4 SFM Information

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 lets you select the starting point in the IGMP SFM Information Table. Clicking the **Refresh** 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 **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The >> button 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
VLAN ID	VLAN ID of the group.
Group	Group address of the group displayed.
Port	Switch port number.
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
Source Address	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
Type	Indicates the Type. It can be either Allow or Deny.
Hardware Filter/Switch	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 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.

2.4.1.64 MLD Snooping

2.4.1.65 MLD Snooping Status

This page provides MLD Snooping status.

The screenshot shows the MLD Snooping Status page. The left sidebar contains a navigation menu with the following items: System Information, Front Panel, Configuration, Monitor, System, Green Ethernet, Ports, DHCP, Security, LACP, Loop Protection, Spanning Tree, MVR, IPMC, IGMP Snooping, MLD Snooping (selected), Status, Groups Information, IPv6 SFM Information, LLDP, MAC Table, VLANs, VCL, sFlow, Redundant Ring&Chain, and DDMI. The main content area displays the MLD Snooping Status page with the following tables:

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-

Object	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	Working Querier Version currently.
Host Version	Working Host Version currently.
Querier Status	Shows the Querier status as "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.
Queries Transmitted	The number of Transmitted Queries.
Queries Received	The number of Received Queries.
V1 Report Received	The number of Received V1 Reports.
V2 Report Received	The number of Received V2 Reports.
V1 Leaves Received	The number of Received V1 Leaves.
Router Port	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 MLD querier. 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.
Port	Switch port number.
status	Indicate whether specific port is a router port or not.

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

2.4.1.66 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 lets you select the starting point in the MLD Group Table. Clicking the **Refresh** 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 **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> button 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
VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port Members	Ports under this group.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically every 3 seconds.
<input type="button" value="Refresh"/>	Refreshes the displayed table starting from the input fields.
<input type="button" value=" <<"/>	Updates the table, starting with the first entry in the MLD Group Table.
<input type="button" value=">>"/>	Updates the table, starting with the entry after the last entry currently displayed.

2.4.1.67 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 lets you select the starting point in the MLD SFM Information Table. Clicking the **Refresh** 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 **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The >> button 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.

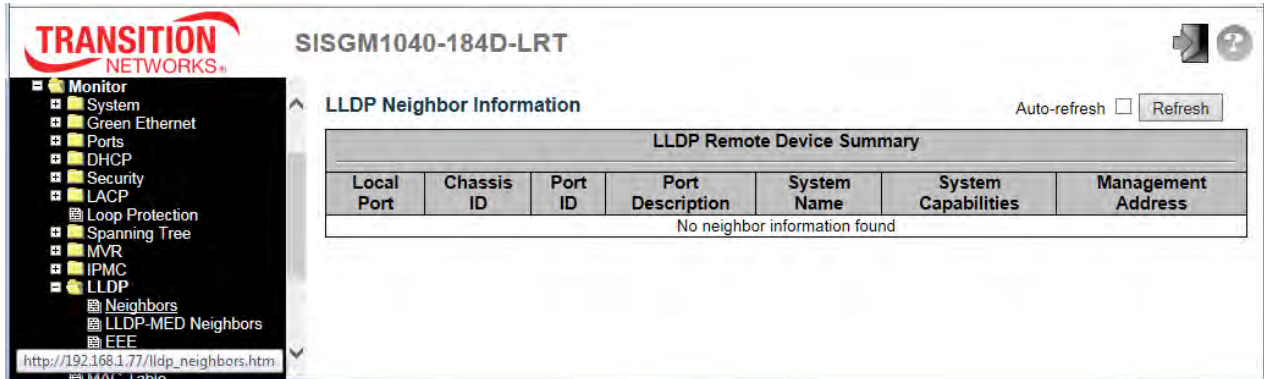
Object	Description
VLAN ID	VLAN ID of the group.
Group	Group address of the group displayed.
Port	Switch port number.
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
Source Address	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
Type	Indicates the Type. It can be either Allow or Deny.
Hardware Filter/Switch	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 every 3 seconds.
<input type="button" value="Refresh"/>	Refreshes the displayed table starting from the input fields..
<input type="button" value=" <<"/>	Updates the table starting from the first entry in the MLD SFM Information Table.
<input type="button" value=">>"/>	Updates the table, starting with the entry after the last entry currently displayed.

2.4.1.68 LLDP

2.4.1.69 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
Local Port	The port on which the LLDP frame was received.
Chassis ID	The Chassis ID is the identification of the neighbor's LLDP frames.
Port ID	The Port ID is the identification of the neighbor port.
Port Description	Port Description is the port description advertised by the neighbor unit.
System Name	System Name is the name advertised by the neighbor unit.
System Capabilities	<p>System Capabilities describes the neighbor unit's capabilities, including:</p> <ol style="list-style-type: none"> 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved <p>When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).</p>

<p>Management Address</p>	<p>Management Address 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>
----------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

2.4.1.70 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
Port	The port on which the LLDP frame was received.
Device Type	<p>LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.</p> <p>LLDP-MED Network Connectivity Device Definition</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"> 1. LAN Switch/Router 2. IEEE 802.1 Bridge 3. IEEE 802.3 Repeater (included for historical reasons) 4. IEEE 802.11 Wireless Access Point 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>LLDP-MED Endpoint Device Definition</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>

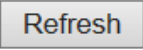
	<p>Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class 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>LLDP-MED Generic Endpoint (Class I)</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>LLDP-MED Media Endpoint (Class II)</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 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>LLDP-MED Communication Endpoint (Class III)</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</p>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>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>
LLDP-MED Capabilities	<p>LLDP-MED Capabilities describes the neighbor unit's LLDP-MED capabilities. The possible capabilities are:</p> <ol style="list-style-type: none"> 1. LLDP-MED capabilities 2. Network Policy 3. Location Identification 4. Extended Power via MDI - PSE 5. Extended Power via MDI - PD 6. Inventory 7. Reserved
Application Type	<p>Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.</p> <ol style="list-style-type: none"> 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. 2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media. 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. 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. 5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. 6. Video Conferencing - for use by dedicated Video Conferencing equipment and

	<p>other similar appliances supporting real-time interactive video/audio services.</p> <p>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.</p> <p>8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media.</p>
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Policy	<p>Policy 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>
TAG	<p>TAG is indicative of whether the specified application type is using a tagged or an 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>
VLAN ID	<p>VLAN ID 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.</p>
Priority	<p>Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).</p>
DSCP	<p>DSCP 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).</p>
Auto-negotiation	<p>Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.</p>
Auto-negotiation status	<p>Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled,</p>

	the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.
Auto-negotiation Capabilities	Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.

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

2.4.1.71 EEE

By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to the fact that the circuits EEE turn off to save power; they need time to boot up before sending traffic over the link.

This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange information about their respective TX and RX "wakeup time", as a way to agree upon the minimum wakeup time they need.

This page provides an overview of EEE information exchanged by LLDP.

Object	Description
Local Port	The port on which LLDP frames are received or transmitted.
Tx Tw	The link partner's maximum time that transmit path can hold-off sending data after deassertion of LPI.
Rx Tw	The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.
Fallback Receive Tw	The link partner's fallback receive Tw. 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.
Echo Tx Tw	The link partner's Echo Tx Tw value. The respective echo values will be defined as the local link partner's 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. 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.

Echo Rx Tw	The link partner's Echo Rx Tw value.
Resolved Tx Tw	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 EEE information exchanged via LLDP).
Resolved Rx Tw	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 EEE information exchanged via LLDP).
EEE in Sync	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 every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.

2.4.1.72 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 for switch SISGM1040-184D-LRT. On the left is a navigation tree with categories like System Information, Configuration, Monitor, and Diagnostics. The main content area is titled 'LLDP Global Counters' and includes a table of global statistics and a section for 'LLDP Statistics Local Counters' with a table of per-port data.

Neighbor entries were last changed	1999-12-31T23:59:58+00:00 (11709 secs. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	371	0	0	0	0	0	0	0
2	5	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	0	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
9	322	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0

Object	Description
Global Counters	
Neighbor entries were last change	Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.
Total Neighbors Entries Added	Shows the number of new entries added since switch reboot.
Total Neighbors Entries Deleted	Shows the number of new entries deleted since switch reboot.
Total Neighbors Entries Dropped	Shows the number of LLDP frames dropped due to the entry table being full.
Total Neighbors Entries Aged Out	Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters	
Local Port	The port on which LLDP frames are received or transmitted.
Tx Frames	The number of LLDP frames transmitted on the port.
Rx Frames	The number of LLDP frames received on the port.
Rx Errors	The number of received LLDP frames containing some kind of error.
Frames Discarded	If a LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP 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 LLDP shutdown frame is received, or when the entry ages out.
TLVs Discarded	Each LLDP 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.
TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value.
Org. Discarded	If LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted.
Age-Outs	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically every 3 seconds.
Refresh	Click to refresh the page immediately.
Clear	Clears the local counters immediately. All counters (including global counters) are cleared upon reboot.

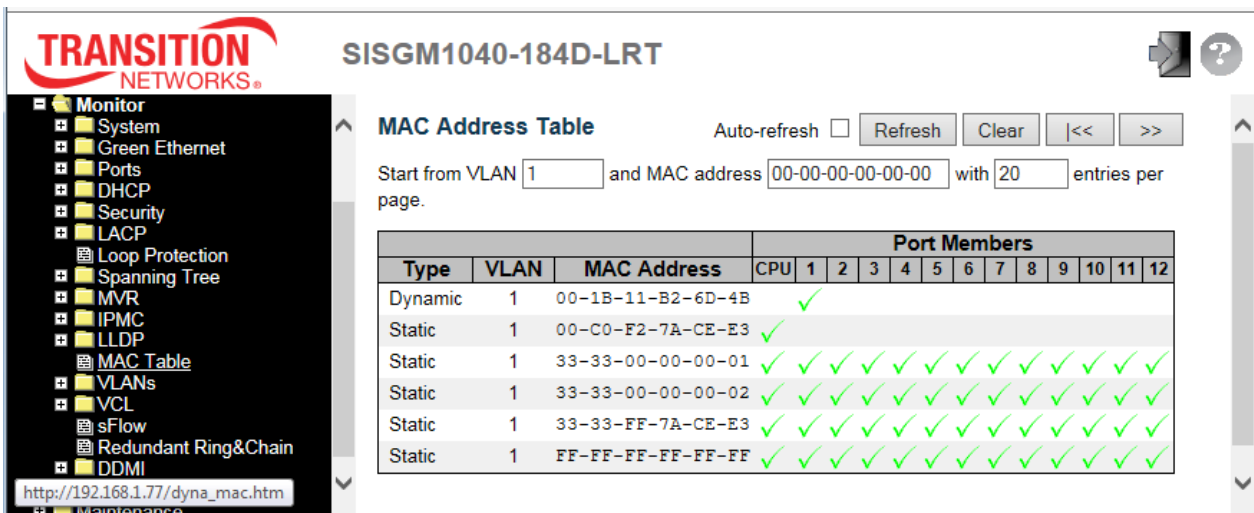
2.4.1.73 MAC Table

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 let you select the starting point in the MAC Table. Clicking the **Refresh** 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 **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.




The >> button 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.



Object	Description
Type	Indicates whether the entry is a static or a dynamic entry.
MAC Address	The MAC address of the entry.
VLAN	The VLAN ID of the entry.
Port Members	The ports that are members of the entry.

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

2.4.1.74 VLANs

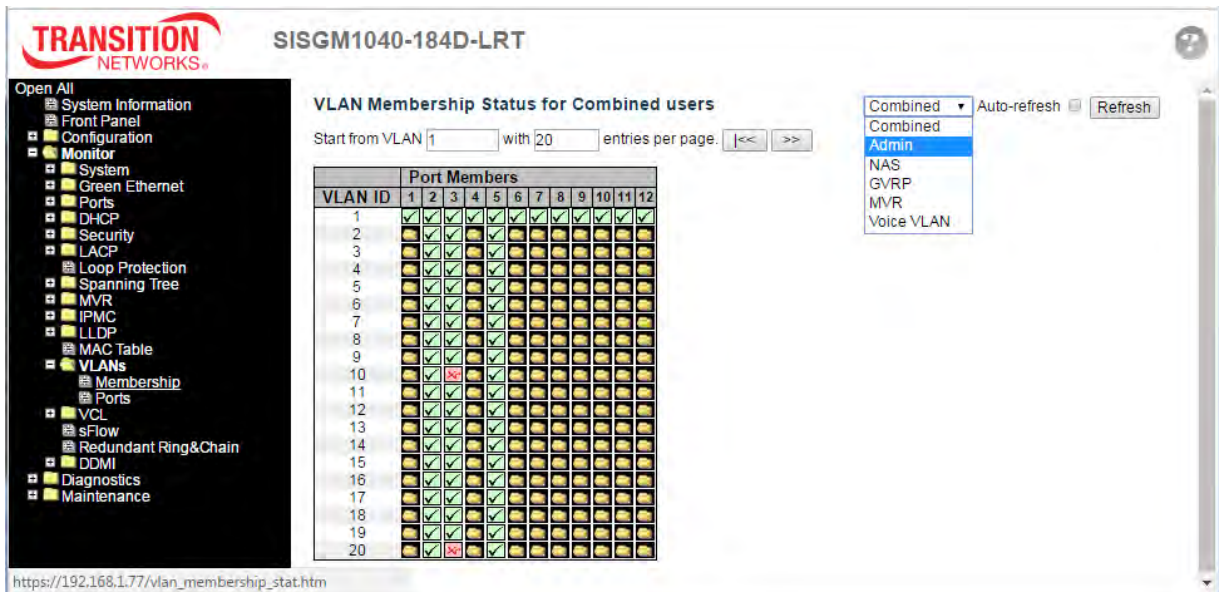
2.4.1.75 VLANs Membership

Each page shows up to 99 entries from the VLAN table (the default is 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 VLAN displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "Start from VLAN" input field lets you select the starting point in the VLAN Table.





Clicking the **Refresh** button will update the displayed table starting from that or the closest next VLAN Table match.

The >> button 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
VLAN User	<p>Various internal software modules may use VLAN services to configure VLAN memberships on the fly. 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 (e.g., Combined, Admin, NAS, GVRP, MVR, Voice VLAN)).</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>

VLAN ID	VLAN ID for which the Port members are displayed.
Port Members	<p>A row of icons (image)s for each port is displayed for each VLAN ID.</p> <p>The image  displays if a port is included in a VLAN.</p> <p>The image  displays if a port is in the forbidden port list.</p> <p>The image  displays 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> <p>The image  displays if a port is not VLAN configured.</p>

Buttons	
<input type="text" value="Combined"/> ▼	Select VLAN Users from this drop down list.
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.

2.4.1.76 VLANs Ports

This page provides VLAN Port Status.

The screenshot shows the 'VLAN Port Status for Combined users' page. The table below represents the data shown in the screenshot:

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	Tag UVID	10	No
2	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
3	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		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
9	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
10	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
11	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
12	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No

Object	Description
VLAN User	<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>
Port	The logical port for the settings contained in the same row.
Port Type	Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port.) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.
Ingress Filtering	Shows whether a given user wants ingress filtering enabled or not. The field is empty if not overridden by the selected user.
Frame Type	Shows the acceptable frame types (All, Tagged, Untagged) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.
Port VALN ID	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.
Tx Tag	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.
Untagged VLAN ID	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 that you want to tag or untag on egress. The field is empty if not overridden by the selected user.
Conflicts	<p>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.</p> <p>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.</p> <p>If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module.</p> <p>The "Combined" user reflects what is actually configured in hardware.</p>

Buttons	
<input type="text" value="Combined"/> ▼	Select VLAN Users from this drop down list (Combined, Admin, NAS, GVRP, MVR, Voice VLAN, MSTP, and VCL).
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.

2.4.1.77 VCL

2.4.1.78 MAC-Based VLAN

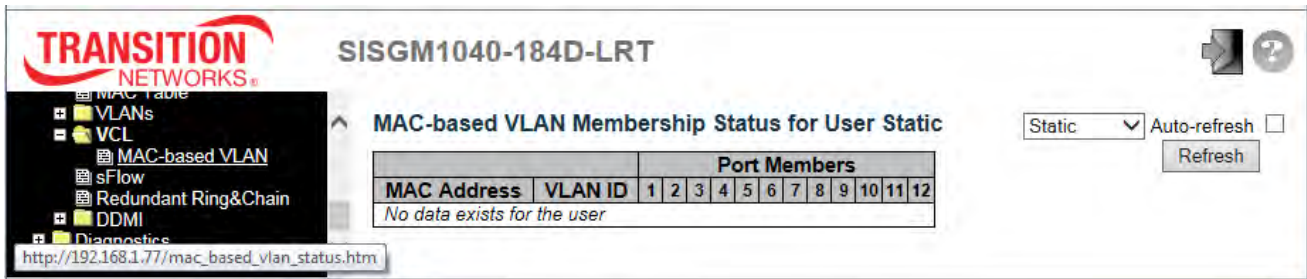
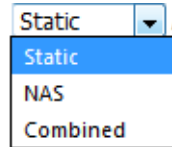
This page shows MAC-based VLAN entries configured by various MAC-based VLAN users.

The following VLAN User types are currently supported:

Static: Refers to CLI/Web/SNMP VLAN user types.

NAS: NAS provides port-based authentication, which involves communications between a Supplicant, an Authenticator, and an Authentication Server.

Combined: Displays the status of all of the User types.



Object	Description
MAC Address	Indicates the MAC address.
VLAN ID	Indicates the VLAN ID.
Port Members	Port members of the MAC-based VLAN entry.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically every 3 seconds.
Refresh	Refreshes the displayed table.

2.4.1.79 sFlow

This page shows receiver and per-port sFlow statistics.

The screenshot displays the web interface for the SISGM1040-184D-LRT device. The left sidebar contains a navigation menu with categories like System Information, Configuration, Monitor, and Diagnostics. The main content area is titled 'sFlow Statistics' and includes a table for 'Receiver Statistics' and a table for 'Port Statistics'. The 'Receiver Statistics' table shows values for Owner, IP Address/Hostname, Timeout, Tx Successes, Tx Errors, Flow Samples, and Counter Samples. The 'Port Statistics' table shows values for Rx Flow Samples, Tx Flow Samples, and Counter Samples for ports 1 through 12. Control buttons for 'Auto-refresh', 'Refresh', 'Clear Receiver', and 'Clear Ports' are visible.

Object	Description
Receiver Statistics	
Owner	<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"> • If sFlow is currently unconfigured/unclaimed, Owner contains <none>. • If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>. • If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.
IP Address/Hostname	The IP address or hostname of the sFlow receiver.
Timeout	The number of seconds remaining before sampling stops and the current sFlow owner is released.
Tx Successes	The number of UDP datagrams successfully sent to the sFlow receiver.
Tx Errors	<p>The number of UDP datagrams that has failed transmission.</p> <p>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</p>

	Web page (Diagnostics > Ping/Ping6).
Flow Samples	The total number of flow samples sent to the sFlow receiver.
Counter Samples	The total number of counter samples sent to the sFlow receiver.
Port Statistics	
Port	The port number for which the following statistics applies.
Rx and Tx Flow Samples	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.
Counter Samples	The total number of counter samples sent to the sFlow receiver originating from this port.

Buttons	
Auto-refresh <input type="checkbox"/>	Check this box to refresh the page automatically every 3 seconds.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.
<input type="button" value="Clear Receiver"/>	Clears the sFlow receiver counters.
<input type="button" value="Clear Ports"/>	Clears the per-port counters.

2.4.1.80 Redundant Ring & Chain Monitoring

This page provides a status overview for all of Ring or Chain status. Ring or Chain configuration is done at the Configuration > Redundant Ring&Chain menu path. The screen below shows no ring or chain enabled.

The screenshot shows the 'Redundant Ring and Redundant Chain Status' page for SISGM1040-184D-LRT. The left sidebar contains a navigation menu with 'Redundant Ring&Chain' selected. The main content area displays a table with the following data:

Group index	Mode	State	Role	Ring Port(s)
1	Disable	--	Ring(Slave)	--
2	Disable	--	Ring(Slave)	--
3	Disable	--	Chain(Member)	--

The screen below shows a ring configured but no chain configured.

The screenshot shows the 'Redundant Ring and Redundant Chain Status' page for SISGM1040-184D-LRT. The left sidebar contains a navigation menu with 'Redundant Ring&Chain' selected. The main content area displays a table with the following data:

Group index	Mode	State	Role	Ring Port(s)
1	Disable	--	Ring(Master)	--
2	Enable	Fail	Ring(Slave)	Port-3(Forward Port, Link Down) Port-4(Forward Port, Link Down)
3	Disable	--	Chain(Member)	--

Object	Description
Group Index	The group index. This parameter is used to easily identify the ring group (1, 2, 3).
Mode	Indicates whether the group is enabled or disabled.
Role	Indicates group is configured as which role (e.g., Ring(Slave) or Chain(Member)).
State	Displays " Normal " when ring is complete. Displays "--" when no ring or chain is configured. Displays " Fail " when ring is incomplete (at least one link is down),.
Ring Port(s)	Describes current status of ring port(s). For example, " <i>Port-1(Forward Port, Link Up, Forwarded)</i> " or " <i>Port-2(Forward Port, Link Down)</i> ".

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

The screen below shows a chain configured but no ring configured.

TRANSITION NETWORKS SISGM1040-184D-LRT

Auto-refresh

Group index	Mode	State	Role	Ring Port(s)
1	Disable	--	Ring(Master)	--
2	Enable	Fail	Ring(Slave)	Port-3(Forward Port, Link Down) Port-4(Forward Port, Link Down)
3	Disable	--	Chain(Member)	--

Navigation menu: LACP, Loop Protection, Spanning Tree, MVR, IPMC, LLDP, MAC Table, VLANs, VCL, sFlow, Redundant Ring&Chain, DDMI, Diagnostics

URL: http://192.168.1.77/tringv2_status.htm

2.4.1.81 DDMI Monitoring

2.4.1.82 Overview

The Monitor > DDMI > Overview page provides global Digital Diagnostic Monitoring Interface (DDMI) information.

Note that DDMI must be enabled at the Configuration > DDMI page for DDMI monitoring to function.

The screenshot shows the 'DDMI Overview' page. The navigation menu on the left includes: IPMVC, IPMC, LLDP, MAC Table, VLANs, VCL, sFlow, Redundant Ring&Chain, DDMI (selected), Overview, Detailed, and Diagnostics. The main content area has the title 'DDMI Overview' and a table with the following data:

Port	Vendor	Part Number	Serial Number	Revision	Date Code	Transceiver
9	Transition	TN-SFP-OC3S	8631044	0000	2007-04-10	100BASE_FX
10	Transition	TN-SFP-OC3M	8630809	0000	2009-11-06	100BASE_FX
11	Transition	TN-SFP-SXD	8886239	0000	2014-10-15	1000BASE_SX
12	Transition	TN-10GSFP-LR1	8800022	0001	2011-08-09	10G

Buttons: Auto-refresh Refresh

Object	Description
Port	The DDMI port number. Click to display the port's detailed information (see the next section below).
Vendor	Indicates Vendor name SFP vendor name (e.g., <i>Transition</i>).
Part Number	Indicates Vendor Part number (PN) provided by SFP vendor (e.g., <i>TN-SFP-SXD</i>).
Serial Number	Indicates Vendor Serial number (SN) provided by vendor (e.g., <i>8672105</i>).
Revision	Indicates Vendor Revision level (rev) for part number provided by vendor (e.g., <i>0000</i>).
Date Code	Indicates Date code Vendor's manufacturing date code (e.g., <i>2009-10-27</i>).
Transceiver	Indicates Transceiver compatibility (e.g., <i>1000BASE_SX</i>).

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

2.4.1.83 Detailed

The Monitoring > DDMI > Detailed page displays detailed SFP Transceiver and DDMI information.

TRANSITION NETWORKS SISGM1040-184D-LRT

Open All / Close All

- System Information
- Front Panel
- Configuration
- Monitor
 - System
 - Green Ethernet
 - Ports
 - DHCP
 - Security
 - LACP
 - Loop Protection
 - Spanning Tree
 - MVR
 - IPMC
 - LLDP
 - MAC Table
 - VLANs
 - VCL
 - sFlow
 - Redundant Ring&Chain
 - DDMI
 - Overview
 - Detailed
 - Diagnostics
 - Maintenance

Transceiver Information Port 9 Auto-refresh Refresh

Vendor	Transition
Part Number	TN-SFP-OC3S
Serial Number	8631044
Revision	0000
Date Code	2007-04-10
Transceiver	100BASE_FX

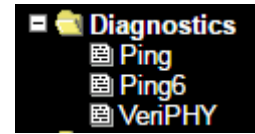
DDMI Information

Type	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)	51.125	90.000	85.000	0.000	-5.000
Voltage(V)	3.3016	3.6000	3.5000	3.1000	3.0000
Tx Bias(mA)	16.928	90.000	70.000	4.000	2.000
Tx Power(dBm)	-10.18	-7.19	-7.99	-13.98	-14.81
Rx Power(dBm)	-14.15	-7.10	-7.96	-30.00	-30.97

http://192.168.1.77/ddmi_detailed.htm

Object	Description
Transceiver Information	
Vendor	Indicates Vendor name SFP vendor name (e.g., <i>Transition</i>).
Part Number	Indicates Vendor Part number (PN) provided by SFP vendor (e.g., <i>TN-SFP-SXD</i>).
Serial Number	Indicates Vendor Serial number (SN) provided by vendor (e.g., <i>8672105</i>).
Revision	Indicates Vendor Revision level (rev) for the part number provided by vendor (e.g., <i>0000</i>).
Date Code	Indicates Date code Vendor's manufacturing date code (e.g., <i>2009-10-27</i>).
Transceiver	Indicates Transceiver compatibility (e.g., <i>100BASE_SX</i>).
DDMI Information	
Current	The current value of temperature, voltage, TX bias, TX power, and RX power.
High Alarm Threshold	The high alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.
High Warn Threshold	The high warn threshold value of temperature, voltage, TX bias, TX power, and RX power.
Low Warn Threshold	The low warn threshold value of temperature, voltage, TX bias, TX power, and RX power.
Low Alarm Threshold	The low alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.

2.5 Diagnostics



2.5.1.1 Ping

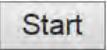
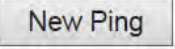
This page lets you issue ICMP PING packets to troubleshoot IP connectivity issues.

1. Navigate to Diagnostics > Ping.
2. Enter the desired IP Address, Ping Length, Ping Count, and Ping Interval.

3. Click the **Start** button.
4. Observe the ICMP Ping Output:

The Ping parameters are described below:

Object	Description
IP Address	The destination IP Address.
Ping Length	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
Ping Count	The count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval	The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Buttons	
	Click to start transmitting ICMP packets.
	Click to re-start diagnostics with PING.


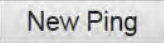
2.5.1.2 Ping6

This page lets you issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

1. Navigate to Diagnostics > Ping6.
2. Enter the desired IP Address, Ping Length, Ping Count, Ping Interval, and Egress Interface.

3. Click the **Start** button.
4. Observe the ICMPv6 Ping Output:

Object	Description
IP Address	The destination IPv6 Address. Must be a valid IPv6 address in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon (:) separating each field.
Ping Length	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
Ping Count	The count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval	The interval of the ICMP packet. Values range from 0 second to 30 seconds.
Egress Interface (only for IPv6)	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

	<p>interface is valid.</p> <p>When an 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.

2.5.1.3 VeriPHY

This page lets you run the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.

1. Navigate to the Diagnostics > Verify menu path.

TRANSITION NETWORKS SISGM1040-184D-LRT

VeriPHY Cable Diagnostics

Port: All

Start

Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	--	--	--	--	--	--	--	--
7	--	--	--	--	--	--	--	--
8	--	--	--	--	--	--	--	--

192.168.1.77/veriphy.htm

2. At the Port dropdown, select **All** ports or individual ports (e.g., **1-8**).
3. Click the **Start** button to run the cable diagnostics. The message “*VeriPhy is running...*” displays momentarily. This will take approximately 5 seconds. If **All** ports are selected, this can take approximately 15 seconds.
4. When completed, the page refreshes automatically; view the cable diagnostics results in the Cable Status table:

TRANSITION NETWORKS SISGM1040-184D-LRT

VeriPHY Cable Diagnostics

Port: All


Start

Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	OK	0	OK	0	OK	0	OK	0
2	OK	0	OK	0	Open	0	OK	0
3	OK	0	OK	0	Open	0	OK	0
4	OK	0	OK	0	OK	0	OK	0
5	OK	0	OK	0	Open	0	OK	0
6	OK	0	OK	0	Open	0	OK	0
7	OK	0	OK	0	OK	0	OK	0
8	OK	0	OK	0	Open	0	OK	0

Note that VeriPHY is only accurate for cables of length 7 - 140 meters. The 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.

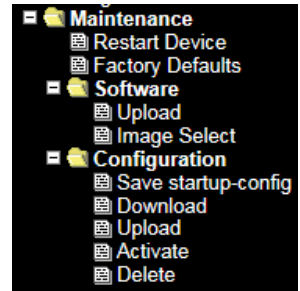
The Cable Status table parameters are described below:

Object	Description
Port	The copper port(s) on which you are requesting VeriPHY Cable Diagnostics (ports 1-8).
Cable Status	<p>Port: Port number.</p> <p>Pair: The status of the cable pair.</p> <p>OK - Correctly terminated pair</p> <p>Open - Open pair</p> <p>Short - Shorted pair</p> <p>Abnormal - incorrect termination</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>Length: The length (in meters) of the cable pair. The resolution is 3 meters</p>

Buttons	
	Click to run the diagnostics.

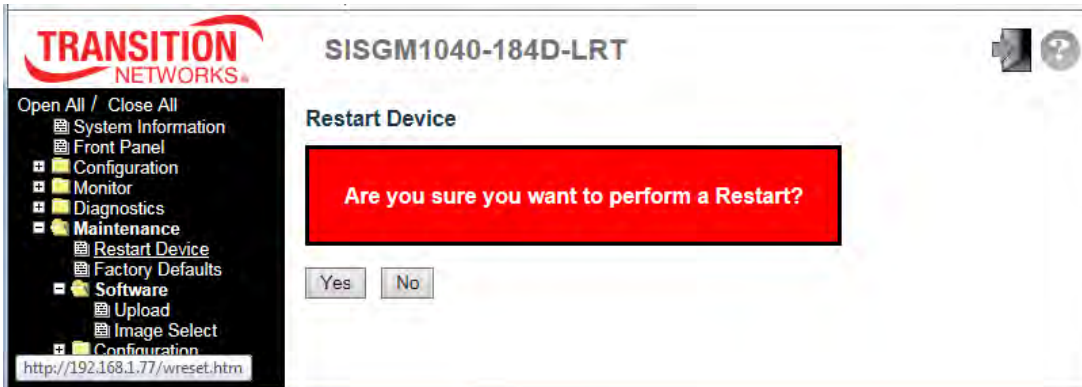
2.6 Maintenance

The Maintenance menu lets you perform restart, reset to factory defaults, software, and Configuration functions.

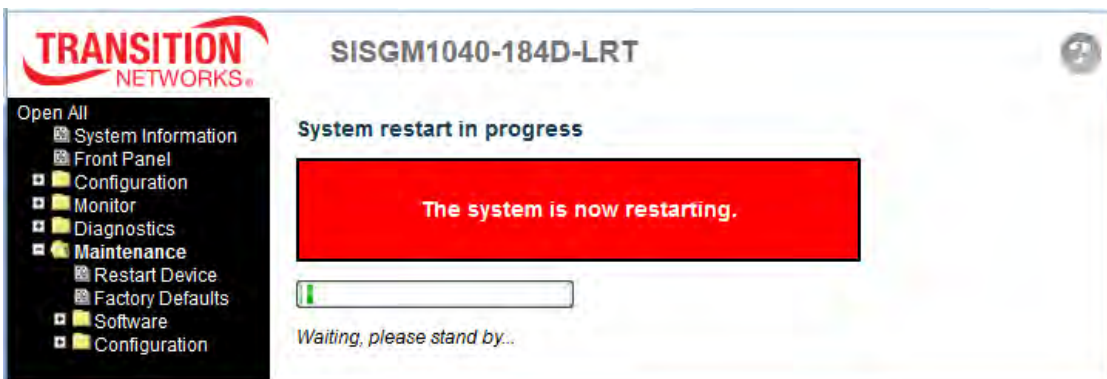


2.6.1.1 Restart Device

You can restart the switch from this page. After restart, the switch will boot normally.

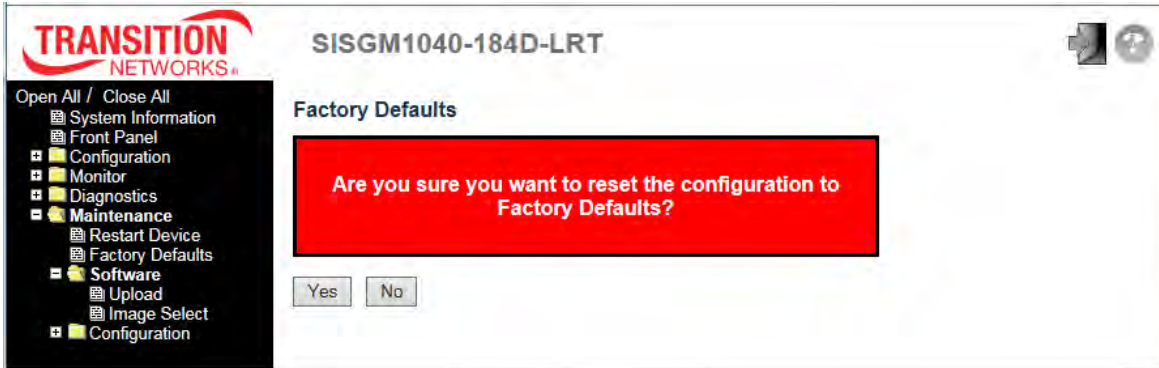


Buttons	
<input type="button" value="Yes"/>	Click Yes to restart the device. The System Information page displays.
<input type="button" value="No"/>	Click No to return to the Port State page without restarting.



2.6.1.2 Factory Default

This page lets you reset the switch configuration to its factory default settings. Only the IP configuration is retained. The new configuration is available immediately, so no restart is necessary.



Buttons	
<input type="button" value="Yes"/>	Click to reset the configuration to Factory Defaults.
<input type="button" value="No"/>	Click to return to the Port State Overview page without resetting the configuration. When done, the message <i>“Configuration Factory Reset Done The configuration has been reset. The new configuration is available immediately.”</i> displays.

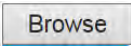



2.6.1.3 Software

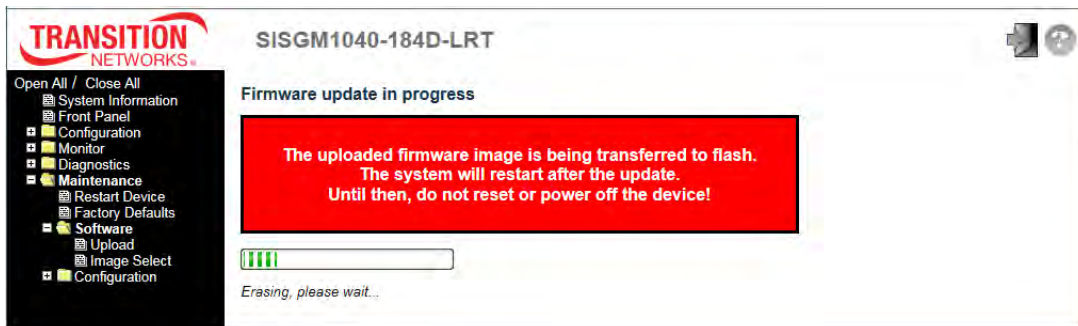
2.6.1.4 Software Upload

The Maintenance > Software > Upload page lets you update the switch firmware.



Buttons	
	Browse to and select the software image file and click the Upload button.
	After selecting the software image, click the Upload 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.

Message: *Firmware update in progress. The uploaded firmware image is being transferred to flash. The system will restart after the update. Until then, do not reset or power off the device!*

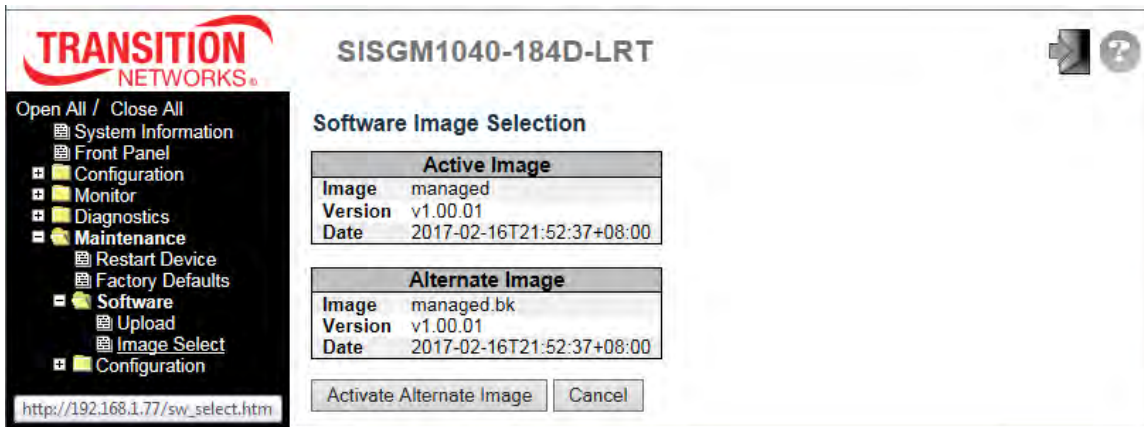


The System Information page displays when the firmware upgrade (Software Upload) is complete. Verify that the Software Version displayed is as expected.

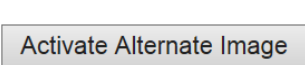

2.6.1.5 Image Select

This page provides information about the active and alternate (backup) firmware images in the device, and lets you 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 and activate this.
3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

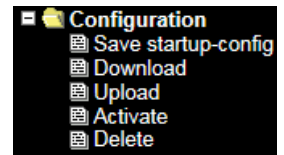


Object	Description
Image	The flash index name of the firmware image. The name of the Active Image is managed , the Alternate Image is named managed.bk .
Version	The version of the firmware image.
Date	The date and time when the firmware was produced.

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.

2.6.1.6 Configuration

The Configuration menu lets you perform Save startup-config, Download Configuration, Upload Configuration, Activate Configuration, and Delete Configuration File functions.



System Files

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch. The three system files are:

running-config	A virtual file that represents the currently active configuration on the switch. This file is volatile.
startup-config	The startup configuration for the switch, read at boot time.
default-config	A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

It is also possible to store up to two other files and apply them to the running-config file, thereby switching configuration.

2.6.1.7 Save startup-config

This copies *running-config* to *startup-config*, thereby ensuring that the currently active configuration will be used at the next reboot.

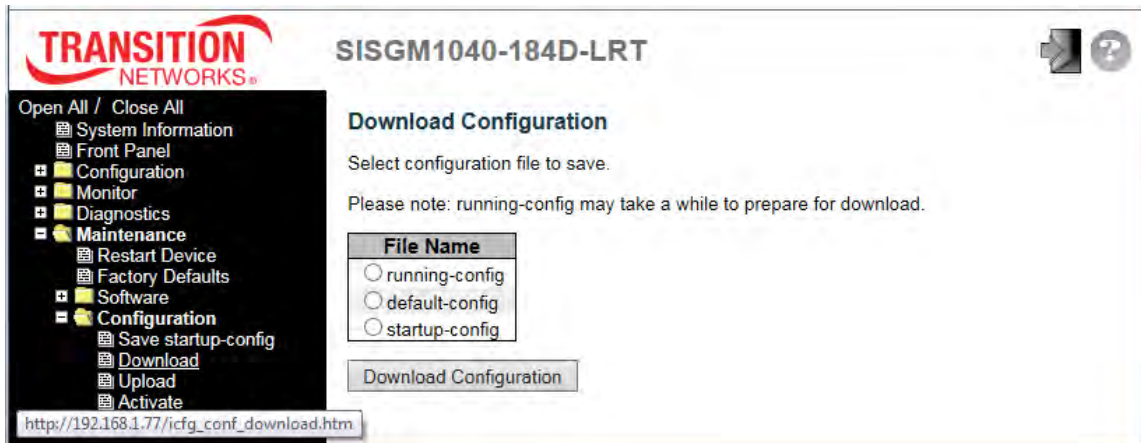


During a **Save Running Configuration to startup-config**, the generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

When done, the message *startup-config saved successfully* displays.

2.6.1.8 Download Configuration

You can download any of the switch files to the web browser. Select a File Name and click the **Download Configuration** button. Downloading the *running-config* file may take a while to complete; the file must be prepared for download.



If a prompt displays like *"Do you want to save startup-config (1.48 KB) from 192.168.1.77"* displays, select **Save**, **Save As**, or **Cancel**, and continue operation.

The file is saved to the default location or to the specified location. You can open the saved file in WordPad or a similar program.

2.6.1.9 Upload Configuration

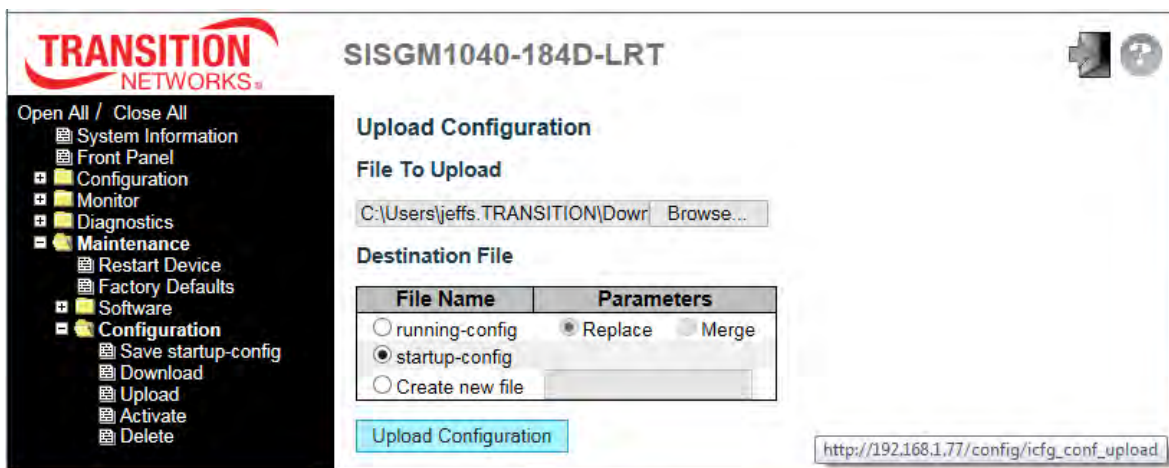
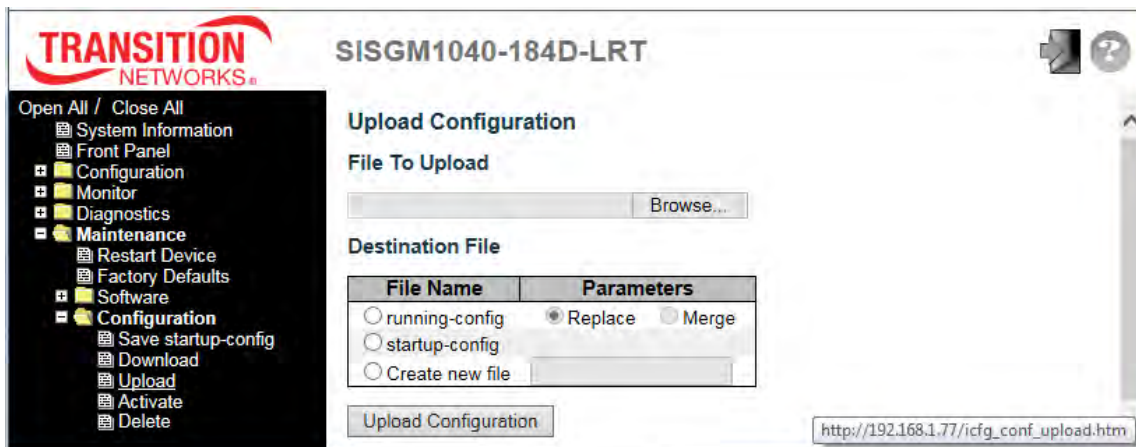
You can upload a file from the web browser to all the files on the switch, except *default-config*, which is read-only. Browse to and select the file to upload, select the destination file on the target, then click the **Upload Configuration** button.

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.



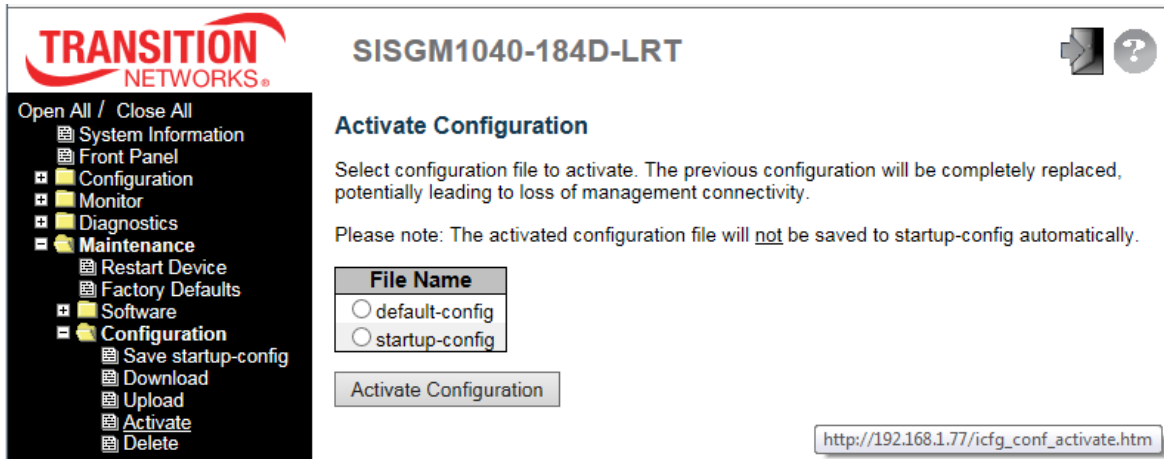
When done, the message *"Upload successfully completed"* displays.

2.6.1.10 Activate Configuration

It is possible to activate any of the configuration files present on the switch, except for *running-config* which represents the currently active configuration.

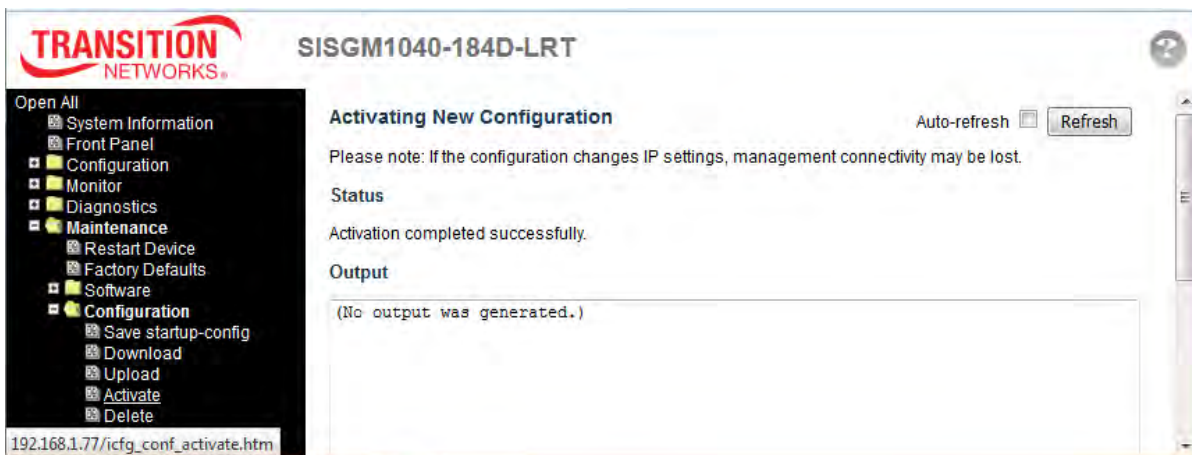
Select the file to activate (*default-config* or *startup-config*) and click the **Activate Configuration** button.

This will initiate the process of completely replacing the existing configuration with that of the selected file.



The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Note: The activated configuration file will not be saved to startup-config automatically.



Note: When activating new configuration, if the configuration changes IP settings, management connectivity may be lost.

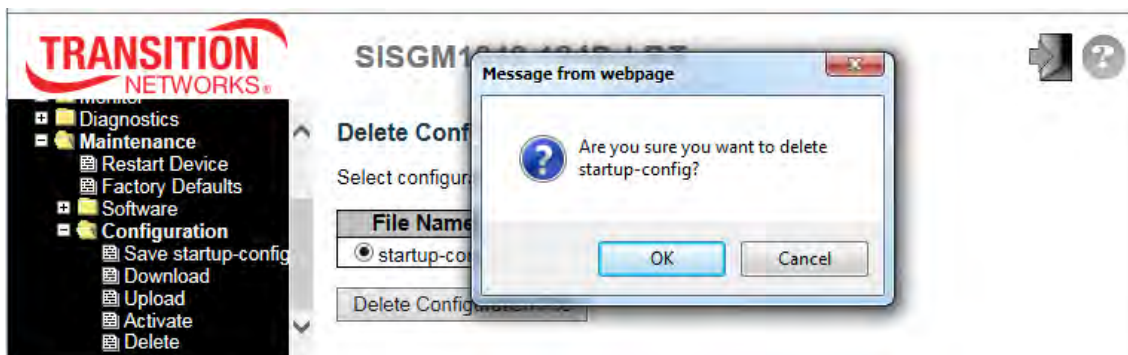
When done, the messages "Status Activation completed successfully." and "(No output was generated.)" display.

2.6.1.11 Delete Configuration File

You can 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 its default configuration.



Select the file to delete and click the **Delete Configuration File** button.



At the confirmation prompt, click the **OK** button to continue or click the **Cancel** button to quit.

The message "*newFileToUpload successfully deleted.*" displays if you clicked **OK**.

3. Technical Specifications

Ethernet	
Operating mode	Store and forward, L2 wire speed/non-blocking switching engine
MAC addresses	8K
Jumbo frames	9K bytes
Copper RJ45 Ports	
Speed	10/100/1000 Mbps
MDI/MDIX Auto-crossover	Support straight or cross wired cables
Auto-negotiating	10/100/1000 Mbps speed auto negotiation; Full and half duplex
Ethernet isolation	1500 VRMS 1 minute
SFP (pluggable) Ports	
Port types supported	SFP (pluggable) Ports 100/1000Base SFP slot
Fiber port connector	Support 100/1000BaseT SFP transceiver LC typically for fiber (depends on module)
Optimal fiber cable	Typical 50 or 62.5/125 μ m for multimode (mm); Typical 8 or 9/125 μ m for single mode (sm)
Network Redundancy	
Fast failover protection rings	Link loss recovery < 20 ms Single and multiple rings supported
Spanning Tree Protocol	IEEE 802.1D STP, IEEE 802.1w RSTP, IEEE 802.1s MSTP
Port Trunk with LACP	Static trunk or Dynamic via LACP (Link Aggregation Control Protocol)
Bridge, VLANs & Protocols	
Flow Control	IEEE 802.3x (Full Duplex) and Back-Pressure (Half Duplex)
VLAN Types	Port-based VLANs; IEEE 802.1Q tag-based VLANs; IEEE 802.1ad Double Tagging (Q in Q) IGMP v1, v2; IGMP Snooping and Querying Immediate leave and leave proxy; Throttling and filtering IEEE 802.1ab Link Layer Discovery Protocol (LLDP)

Traffic Management and QoS	
Priority	IEEE 802.1p QoS
Number of queues per port	8
Scheduling schemes	SPQ, WRR
Traffic Shaper	Port-based shaping
Security	
Port security	IP- and MAC-based access control
Power	
Power input	Redundant Input Terminals
Input voltage range	12-58 VDC
Max. power consumption	10.5W
Reverse power protection	Yes
Transient protection	> 15,000 watts peak
LED Indicators	
Power Status indication	Indication of power input status
Ethernet port indication	Link and Speed
Management	
User Management Interface	CLI (Command Line Interface) Web-based Management SNMP v1, v2c Telnet (5 sessions)
Management Security	HTTPS, SSH, RADIUS client for Management
Upgrade and Restore	Configuration import / Export Firmware Upgrade
Diagnostics	Syslog Per-VLAN Mirroring SFP with DDM (Digital Diagnostic Monitoring)
MIBs	RMON 1, 2, 3, 9; Q-Bridge MIB, RFC 1213 MIB-II, RFC 4188 Bridge
DHCP	Client, Server, Relay, Snooping, Option 82
NTP/SNTP	Yes

Environmental & Compliance	
Operating temp. range	-40 to +75 °C (cold startup at -40 °C)
Storage temp. range	-40 to +85 °C
Humidity (non-condensing)	5 to 95% RH
Vibration, shock & freefall	IEC68-2-6, -27, -32
Certification compliance	CE/FCC; EN50121-4
Electrical safety	CSA C22, EN61010-1, CE
EMC	FCC Part 15, CISPR 22 (EN55022) Class A IEC 6100-4-2, -3, -4, -5, -6
RoHS and WEEE	RoHS Pb free and WEEE compliant
MTBF	> 25 years
Mechanical	
Ingress protection	IP30
Installation options	DIN-Rail mount, Wall mount
Dimensions	154 mm x 109 mm x 60 mm
Weight	1056 g (2.32 lbs.)

System Statistics	Maximum System Value
VLAN IDs	4096
VLAN Limitation	1024
User Privilege Levels	15
RMON Statistics Entries	65, 535
RMON Alarm Entries	65
RMON Event Entries	65, 535
IPMC Profiles	64
IPMC Rules / Address Entries	128
ACEs	256
ICMP Types / Codes	255
RADIUS Servers	5
TACACS+ Servers	5

MAC-based VLAN Entries	256
IP subnet-based VLAN Entries	128
Protocol-based VLAN Groups	125
Voice VLAN OUIs	16
QCEs	256
IP Interfaces	8
IP Routes	32
Security Access Management	16
MVR VLANs	4
MAC Learning table addresses	8K
IGMP Groups	256

MIBs Supported

1. RFC 1213: Management Information Base for Network Management of TCP/IP-based internets: MIB-II
2. RFC 2819: Remote Network Monitoring Management Information Base
3. RFC 2863: The Interfaces Group MIB
4. RFC 3411: An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
5. RFC 3412: Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
6. RFC 3414: User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
7. RFC 3415: View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
8. RFC 3621: Power Ethernet MIB
9. RFC 3635: Definitions of Managed Objects for the Ethernet-like Interface Types
10. RFC 3636: Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)
11. RFC 4133: Entity MIB (Version 3)
12. RFC 4188: Definitions of Managed Objects for Bridges
13. RFC 4292: IP Forwarding Table MIB
14. RFC 4293: Management Information Base for the Internet Protocol (IP)
15. RFC 4363: Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions

4. Service, Warranty, and Tech Support

See the *SISGM1040-184D-LRT Install Guide* for related information.

5. Compliance Information

See the *SISGM1040-184D-LRT Install Guide* for related information.

Glossary

A

ACE

An ACE (Access Control Entry) describes access permission associated with a particular ACE ID. There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL

ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are 3 web-pages associated with manual ACL configuration:

ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web page help text for each specific port property.

ACL|Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES

AES is an acronym for **A**dvanced **E**ncryption **S**tandard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

Aggregation

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability. (Also *Port Aggregation, Link Aggregation*).

ARP

ARP is an acronym for **A**ddress **R**esolution **P**rotocol. It is a protocol that used to convert an **IP** address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CDP

CDP is an acronym for **C**isco **D**iscovery **P**rotocol.

D

DDMI

DDMI is an acronym for **D**igital **D**iagnosics **M**onitoring **I**nterface. It provides an enhanced digital diagnostic monitoring interface for optical transceivers which allows real time access to device operating parameters.

DEI

DEI is an acronym for **D**rop **E**ligible **I**ndicator. It is a 1-bit field in the VLAN tag.

DES

DES is an acronym for **D**ata **E**ncryption **S**tandard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP is an acronym for **D**ynamic **H**ost **C**onfiguration **P**rotocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number. The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Server

DHCP Server is used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP client.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

DNS is an acronym for **D**omain **N**ame **S**ystem. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets. An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

Drop Precedence Level

Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level. A DP level of 0 (zero) corresponds to 'Committed' (Green) frames and a DP level of 1 corresponds to 'Discard Eligible' (Yellow) frames.

DSCP

DSCP is an acronym for **D**ifferentiated **S**ervices **C**ode **P**oint. It is a field in the header of **IP** packets for packet classification purposes.

E

ECE

ECE is EVC Control Entries. These rules are ordered in a list to control the preferred classification.

EEE

EEE (Energy Efficient Ethernet) is defined in IEEE 802.3az.

EPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

F

FTP

FTP is an acronym for **F**ile **T**ransfer **P**rotocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

Fast Leave

Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

H

HTTP

HTTP is an acronym for **H**ypertext **T**ransfer **P**rotocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW). HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for **H**ypertext **T**ransfer **P**rotocol over **S**ecure Socket Layer. It is used to indicate a secure HTTP connection. HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP). SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP is an acronym for **I**nternet **C**ontrol **M**essage **P**rotocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for **I**nternet **G**roup **M**anagement **P**rotocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier. There will be only one IGMP Querier that wins Querier election on a particular link.

IP

IP is an acronym for **I**nternet **P**rotocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for **IP MultiCast**. IPMC supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6.

IPMC Profile

IPMC Profile is an acronym for **IP MultiCast Profile**. IPMC Profile is used to deploy the access control on IP multicast streams.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The **Link Aggregation Control Protocol**, allows bundling several physical ports together to form a single logical port.

LLC

The IEEE 802.2 **Logical Link Control** (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

LLDP

LLDP is an IEEE 802.1ab standard protocol. The **Link Layer Discovery Protocol** (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LLQI

LLQI (Last Listener Query Interval) is the maximum response time used to calculate the Maximum Response Code inserted into Specific Queries. It is used to detect the departure of the last listener for a multicast address or source. In IGMP, this term is called LMQI (Last Member Query Interval).

LOC

LOC is an acronym for **L**oss **O**f **C**onnectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS.

M

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

MD5

MD5 is an acronym for **M**essage-**D**igest algorithm **5**. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for **M**ulticast **L**istener **D**iscovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MLD Querier

A router sends MLD Query messages onto a particular link. This router is called the Querier. There will be only one MLD Querier that wins Querier election on a particular link.

MSTP

In 2002, the IEEE introduced an evolution of RSTP: the **M**ultiple **S**panning **T**ree **P**rotocol. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The standard was originally defined by IEEE 802.1s, but was later incorporated in IEEE 802.1D-2005.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them (Wikipedia).

N

NAS

NAS is an acronym for **N**etwork **A**ccess **S**erver. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NTP

NTP is an acronym for **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

Optional TLVs

An LLDP frame contains multiple TLVs. For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

P

PCP

PCP is an acronym for **P**riority **C**ode **P**oint. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).

PING

ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

Private VLAN

In a private VLAN, PVLANS provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

PTP

PTP is an acronym for **P**recision **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems.

Q

QCE

QCE is an acronym for **Q**oS **C**ontrol **E**ntry. It describes QoS class associated with a particular QCE ID. There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

QCL is an acronym for **Q**oS **C**ontrol **L**ist. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects. Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QoS

QoS is an acronym for **Q**uality **o**f **S**ervice. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

QoS class

Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

Querier Election

Querier election is used to dedicate the Querier, the only one router sends Query messages, on a particular link. Querier election rule defines that IGMP Querier or MLD Querier with the lowest IPv4/IPv6 address wins the election.

R

RARP

RARP is an acronym for **R**everse **A**ddress **R**esolution **P**rotocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for **R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

Router Port

A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the **R**apid **S**panning **T**ree **P**rotocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

sFlow

sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector. Additional information can be found at <http://sflow.org>.

SHA

SHA is an acronym for **S**ecure **H**ash **A**lgorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SNAP

The **S**ub**N**etwork **A**ccess **P**rotocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP is an acronym for **S**imple **N**etwork **M**anagement **P**rotocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for **S**imple **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SSH

SSH is an acronym for **S**ecure **S**Hell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

STP

Spanning **T**ree **P**rotocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

T

TACACS+

TACACS+ is an acronym for **T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem **P**lus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

TCP

TCP is an acronym for **T**ransmission **C**ontrol **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers. The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for **T**ELEtype **N**ETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for **T**rivial **F**ile **T**ransfer **P**rotocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

TLV

TLV is an acronym for **T**ype **L**ength **V**alue. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

U

UDP

UDP is an acronym for **U**ser **D**atagram **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact. Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UPnP

UPnP is an acronym for **U**niversal **P**lug and **P**lay. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

V

VLAN

Virtual LAN. A method to restrict communication between switch ports. At layer 2, the network is partitioned into multiple, distinct, mutually isolated broadcast domains.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, you can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

W

WRED

WRED (**W**eighted **R**andom **E**arly **D**etection) is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DP level is used as input to WRED. A higher DP level assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

WTR

WTR is an acronym for **W**ait **T**o **R**estore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is done.



Transition Networks

10900 Red Circle Drive

Minnetonka, MN 55343 USA

tel: +1.952.941.7600 | toll free: 1.800.526.9267 | fax: 952.941.2322

sales@transition.com | techsupport@transition.com | customerservice@transition.com

Copyright© 2017 Transition Networks. All rights reserved. Printed in the U.S.A.

SISGM1040-184D-LRT Web User Guide 33710 Rev. A