AMG

9IM2x/9HM2x User Manual

User Manual AMG 9IM2x/9HM2x

Version No : 2.1.7

employees and Agents will not be responsible for any loss, however arising, from the use of, or reliance on, this information.

Legal Notice: Parts of this product are protected by patents.

Electromagnetic Compatibility (EMC)

This is a Class B product.

Manufacturer's Declaration of Conformance

A Declaration of Conformity in accordance with the following EU standards has been made and is kept on file at the address shown on the last page.

The manufacturer declares that the product supplied with this document is compliant with the provisions of the EMC Directive 2014/30/EU, the Low Voltage Directive LVD 2006/95/EC and the CE Marking Regulation 768/2008/EC & Decision 765/2008.

This device complies with Part 15 of the FCC Rules.
Operation of this product is subject to the following two conditions:
This device may not cause harmful interference.
This device must accept any interference received, including interference that may cause undesired operation.

ICES-003
This Class B digital apparatus meets all requirements of the Canadian Interference causing equipment regulations.

Cet appareil numérique de la Classe B Respecte toutes les exigences du Règlement sur le matérial rouiller du Canada.

Before You Begin

Read these instructions carefully before installing or operating this product.

Note: This equipment should be installed by a qualified service person and should conform to local and national regulations.

This manual provides installation and operation information. To use this document you must have the following minimum qualifications

- A basic knowledge of Ethernet, Ethernet Switches and Layer2 networking.
- A basic knowledge of electrical wiring and low-voltage electrical connection.

Intended Use

Use this product only for the purpose for which it was designed, as described in this manual.

Warning:
Improper use of this equipment can cause severe bodily injury or equipment damage

---

Environmental Conditions

Storage: -45° to +85° C. The switch should be allowed to acclimatize to its operational temperature range before power is supplied. Additionally, if the switch is moved from a colder area to a warmer area, precautions should be taken to ensure that condensation is prevented.

Operational: -40° to +74° C.

Customer Support

For assistance in installing, operating, maintaining and troubleshooting this product, please refer to this document and any other documentation provided. If you still require assistance, please contact AMG Systems at the address shown on the last page

Change History

Document Rev No.	Change Description	Author	Date
2.0.0.5	Draft	M.I.Steval	22-04-2016
2.0.0.6	1. New non-TFTP s/w upgrade feature. 2. Updated screen-capture examples	M.I.Steval	16-06-2016
2.0.0.b7	Beta7 Release	M.I.Steval	01/07/2016
2.0.0.b8	1. Clarification of configuration in var sections 2. Added SFP transceivers section	M.I.Steval	13/07/2016
2.0.0.b9	1. Corrected rear panel DC power options 2. Clarification of configuration in various sections 3. IPv4 Default DHCP settings 4. Details of Syslog Traps and Messages 5. ECFM Module documentation added. 6. Updated EMC Directive Spec. 7. Static Unicast / Multicast Address added. 8. Updated LLDP section	M.I.Steval	08/09/2016
2.0.0	Release version 1. Management feature : additional user / password. 2. Updated screen captures VLANs, LLDP, RSTP 3. Updated Save and Restore section.	M.I.Steval	13/10/2016
2.1.0	Release version for 9IM2x/9HM2x platform Provisional.	M.I.Steval	11/01/2017
2.1.1	Unreleased draft feature updates	M.I.Steval	23/02/2017
2.1.4	1. Additional Features : DHCP Server IGMP Snooping Jumbo Frame Support High Speed I/O 2. Updated Screenshots. 3. Added 240W info.	M.I.Steval	19/07/2017
2.1.4.1	1. Correction VLAN Chapter heading missing. 2. Minor corrections to RSTP & MSTP configuration. 3. Carifications in SNMP Trap Manager configuration.	M.I.Steval	10/08/2017
2.1.5.3	1. User definable management VLAN. 2. SFP Transceiver Diagnostics.	M.I.Steval	30/10/2017
2.1.6	Serial Data I/O and Contact Closures - new variants	M.I.Steval	09/04/2018
2.1.7	1. SNMP minor clarifications. 2. PoE Power monitoring and control. 3. SFP Expander additional SFP ports	M.I.Steval	24/06/2018

Contents

Figures

Tables

Definitions and Acronyms

Acronyms Used in this Document

Acronym	Explanation
ACL	Access Control List
API	Application Programming Interface
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
BPS	Bits-Per-Second
CBP	Customer Backbone Port
CE	Customer Edge
CFA	Common Forwarding Agent
CFM	Connectivity Fault Management
CIDR	Classless Inter Domain Routing
CIST	Common Internal Spanning Tree
CLI	Command Line Interface
CoS	Class of Service
CoSQ	Class of Service Queues
CRC	Cyclic Redundancy Check
C-VID	Customer VLAN ID
C-VLAN	Customer VLAN
DB	Database
DHCP	Dynamic Host Configuration Protocol
DM	Delay Measurement
DNS	Domain Name System
DR	Designated Router
DST	Daylight Saving Time
DVMRP	Distance Vector Multicast Routing Protocol
ECFM	Ethernet Connectivity Fault Management
ESP	Encapsulating Security Payload
FDB	Forwarding Database

Acronym	Explanation
GARP	Generic Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
GRE	Generic Routing Encapsulation
GVRP	GARP VLAN Registration Protocol
HMAC	Hash-based Message Authentication Code
HTTP	Hyper Text Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IGS	IGMP Snooping
IP	Internet Protocol
IPv4	IP version 4
ISL	Inter-Switch Link
IST	Internal Spanning Tree
ITU	International Telecommunication Union
IVL	Independent VLAN Learning
IVR	Inter VLAN Routing
L2	Layer2
L2F	Layer2 Forwarding
L2GP	Layer2 Gateway Port
L3	Layer3
L4	Layer 4
LA	Link Aggregation
LACP	Link Aggregation Control Protocol
LACPDU	LACP Data Unit
LAN	Local Area Network
LDP	Label Distribution Protocol

Acronym	Explanation
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLTD	Link Layer Topology Discovery
MA	Maintenance Association
MAC	Media Access Control
MAN	Metropolitan Area Network
MAU	Medium Attachment Unit
MD	Maintenance Domain
ME	Maintenance Entity
MEG	Maintenance Entity Group
MEN	Metro Ethernet Network
MEP	Maintenance End Point
MI	Multiple Instance
MIB	Management Information Base
MLD	Multicast Listener Discovery
MLDS	Multicast Listener Discovery Snooping
MP	Message Processing
MPLS	Multi-Protocol Label Switching
MRP	Multiple Registration Protocol
MSR	MIB Save and Restore
MST	Multiple Spanning Tree
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NMS	Network Management System
NTP	Network Time Protocol
NVRAM	Non Volatile Random Access Memory
OSI	Open System Interconnection
OUI	Organization Unique Identifier

Acronym	Explanation
PCB	Provider Core Bridge
PDU	Protocol Data Unit
PEB	Provider Edge Bridge
PID	Protocol Identifier
PIM	Protocol Independent Multicasting
PIP	Provider Instance Port
PNP	Provider Network Port
PPP	Point to Point Protocol
PTETID	Provider Backbone Bridging – Traffic Engineering Multiple Spanning Tree ID
PVID	Port VLAN ID
PVRST	Per VLAN Rapid Spanning Tree
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RARP	Reverse Address Resolution Protocol
RDI	Remote Defect Indication
RIB	Routing Information Base
RIP	Routing Information Protocol
RM	Redundancy manager
RP	Rendezvous Point
RSTP	Rapid Spanning Tree Protocol
SA	Source-Active
SEM	State Event Machine
SFTP	SSH File Transfer Protocol
SHA	Security Hash Algorithm
SM	Sparse Mode
SMTP	Simple Mail Transfer Protocol
SNAP	Sub Network Access Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSH	Secure Shell

Acronym	Explanation
SSL	Secure Socket Layer
SST	Single Spanning Tree
STP	Spanning Tree Protocol
SVL	Shared VLAN Learning
S-VLAN	Service VLAN
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TELNET	Telecommunications Network
TFTP	Trivial File Transfer Protocol
TLV	Type, Length, Value
TTL	Time-To-Live
UDP	User Datagram Protocol
UNI	User Network Interface
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VC	Virtual Circuit
VID	VLAN ID
VLAN	Virtual LAN
WAN	Wide Area Network

Chapter 1

Introduction

This user's guide is targeted to provide information on installing, configuring and maintaining the **AMG 9IM2x/9HM2x** Multi-service Ethernet switches.

AMG 9IM2x/9HM2x Multi-Service Ethernet Switch has all capabilities to support ruggedized Layer2 Managed Ethernet functionality. In addition to Layer2 & some Layer3 functionality, these products also support integration of low-speed I/O, allowing Serial Ports, Alarm Contacts, Audio Devices and Analogue Video to be directly connected to the switch, without requirement for any additional hardware.

Historically, this requirement has been dealt with through the use of third-party serial port, audio, and Contact-closure I/O servers, resulting in a disparate, multi-vendor product mix and corresponding issues with product integration. **AMG 9IM2x/9HM2x** Multi-Service Ethernet switches eliminate all these issues with a one-box solution. These switches offer a common web management interface for configuration of all aspects of the device - Ethernet as well as serial ports, audio ports and Alarm I/O.

The AMG 9IM2x/9HM2x management features are designed to minimize administrative management effort, while enhancing and improving network traffic control.

AMG 9IM2x/9HM2x supports easy management and configuration through SNMP, CLI or WEB GUI.

1.1 AMG 9IM2x/9HM2x Models

This section describes different hardware configuration examples of **AMG 9IM2x/9HM2x** series products.

All systems are available as DIN Rail mounting units.

Part numbers	Description
AMG9IM2-8G-2S	21hp : 8x RJ45 GbE + 2x SFP GbE
AMG9IM2-4FH-1S-4S16C	14hp : 4x RJ45 FE + 1x SFP GbE/FE + 4x Serial Data + 16 Contact Closures + PoE/+
AMG91IM2-20GH-5S-4S16C-P240	42hp : 20x RJ45 GbE + 5x SFP GbE/FE + 4x Serial Data + 16 Contact Closures

Table 1-1 : AMG9IM2x Model Examples

Front panels of this system are depicted as shown in following pages:

NOTE : Please see separate User Guide for AMG Video Encoder

1.2 AMG9IM2-8G-2S

21hp : 8x RJ45 GbE + 2x SFP GbE

Figure 1-1 : 9IM2-8G-2S

1.3 AMG91IM2-4FH-1S-4S16C

14hp : 4x FE (4 PoE+) + 4x serial + 16x contact closures + 1x SFP GbE/FE

Figure 1-2 : 91IM2-4FH-1S-4S16C

1.4 AMG91IM2-20GH-5S-4S16C-P240

42hp : 20x GbE + 4x serial + 16x contact closures + 5x SFP GbE/FE

Figure 1-3 : 91IM2-20GH-5S-4S16C-P240

Chapter 2

Hardware Description

This section describes **AMG 9IM2x/9HM2x** hardware. It describes how the different ports, LEDs and connectors are to be used.

AMG 9IM2x/9HM2x has ports for connectivity to different devices. These ports can be categorized into 3 categories

Console port – RJ45 serial RS-232 data for access to CLI (Command Line) interface.

Ethernet ports – used for Ethernet connectivity. These ports can be copper ports or Transceiver ports. Copper ports can operate at speeds of 10/100/1000 Mbps. Transceiver ports can accommodate optical connectivity through Fibre transceivers as well as copper connectivity through copper transceivers.

I/O Ports – This product series has support for built-in I/O ports in order to accommodate serial data ports, alarm contacts, audio devices and video encoder ports without requirement for any additional hardware.

AMG 9IM2x/9HM2x has LEDs on the front panel to indicate status and activities of different ports in the system.

Use the following hyperlinks to view the various hardware features:

2.1 Management Console

Console port – RJ45 serial RS-232 data for access to CLI (Command Line) interface. Management of M-SES from PC using serial terminal application such as PuTTY, Hyperterminal etc. is possible using RJ45 to DB9 Adaptor / Cable provided.

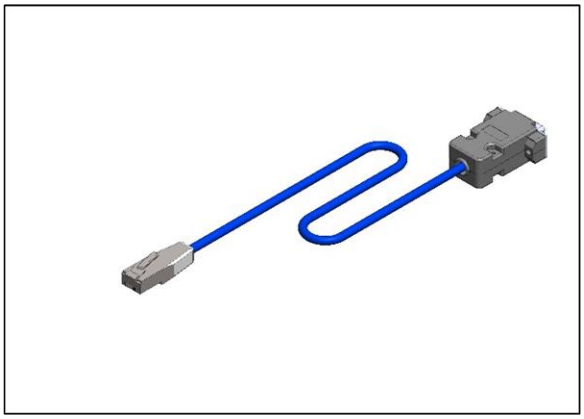


Figure 2-1 : Console Adaptor / Cable

Console connections are provide using supplied AMG RJ45 to DB9 Adaptor. This provides a direct connection to a PC's DB9 serial port using a "straight-though" Ethernet patch cable.

Note. only DB9 pins 2,3,5 are actually used – but all wires are connected in the adaptor as shown in the following table:

RJ45 Cable Colour T568B	AMG RJ45 Pin No.	RJ45 RS232 Signal	RJ45 DCE Wire Colour	DB9 RS232 Pin No.	PC DTE RS-232 Signal
White/Orange	1	n/c	Blue	1	DCD
Orange	2	Tx-OUT	Orange	2	Rx-IN
White/Green	3	Rx-IN	Black	3	Tx-OUT
Blue	4	n/c	Red	4	DTR
White/Blue	5	GND	Green	5	GND
Green	6	n/c	Yellow	6	DSR
White/Brown	7	n/c	Brown	7	RTS
Brown	8	n/c	White	8	CTS

Table 2-1 : Console Port Connections

2.2 Ethernet Connections

Ports P1 to P24 have RJ45 connectors providing 10/100/1000Mbps.

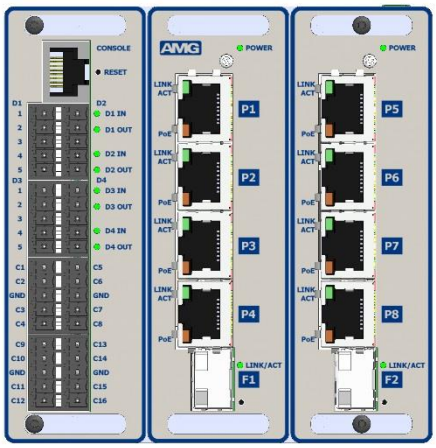


Figure 2-2 : RJ45 Ethernet Ports

Ports F1 to F6 and FA to FC are SFP transceiver ports for use with fibre or copper SFPs. For further details see tables below.

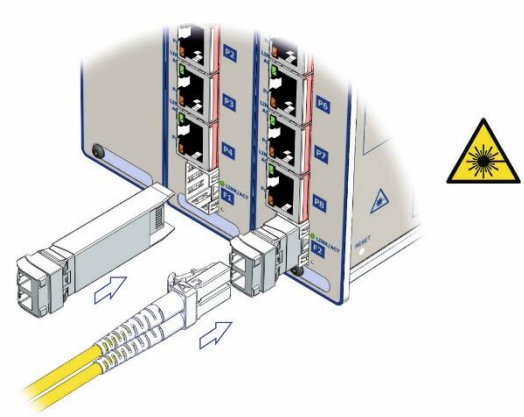


Figure 2-3 : SFP Transceiver Ports

Singlemode Fibre

AMG Part Numbers	Ports Supported	Fibre Type	Wavelength Tx (nm)	Speed (Mbps)	Max distance
S18074	F1-F6, FC	dual fibre	1310	100	20km
S18170	F1-F6, FC	dual fibre	1310	100	40km
S18056	F1-F6, FA-FC	dual fibre	1310	1000	20km
S18057	F1-F6, FA-FC	dual fibre	1550	1000	40km
S18054/55	F1-F6, FA-FC	single fibre	1310/1550	1000	40km

Table 2-2 : Singlemode Fibre SFPs

Multi-Mode Fibre

AMG Part Numbers	Ports Supported	Fibre Type	Wavelength Tx (nm)	Speed (Mbps)	Max distance
S18082	F1-F6, FC	dual fibre	1310	100	2km
S18095/96	F1-F6, FC	single fibre	1550/1310	100	2km
S18200/201	F1-F6, FA-FC	single fibre	1550/1310	1000	500m

Table 2-3 : Multi-mode Fibre SFPs

Copper

AMG Part Numbers	Ports Supported	Connector Type	Speed (Mbps)	Max distance
S24010	F1-F6, FC	RJ45	10/100/1000	100m
S24010	F1-F6, FC	RJ45	1000	100m

Table 2-4 : Copper SFPs

Note: for unsupported transceivers AMG 9IM2x/9HM2x Management Interface gives the provision to configure the speed manually.

2.3 I/O Connections

For low speed serial data ports (RS-232/RS-485/RS-422) and other I/O, the device provides up to 8x 5-way connectors depending on the model variant.

Each connector is a Phoenix style connector providing a total of 4x Bi-Directional low speed data ports D1-D4 and 16x configurable contact closure ports C1-C16.

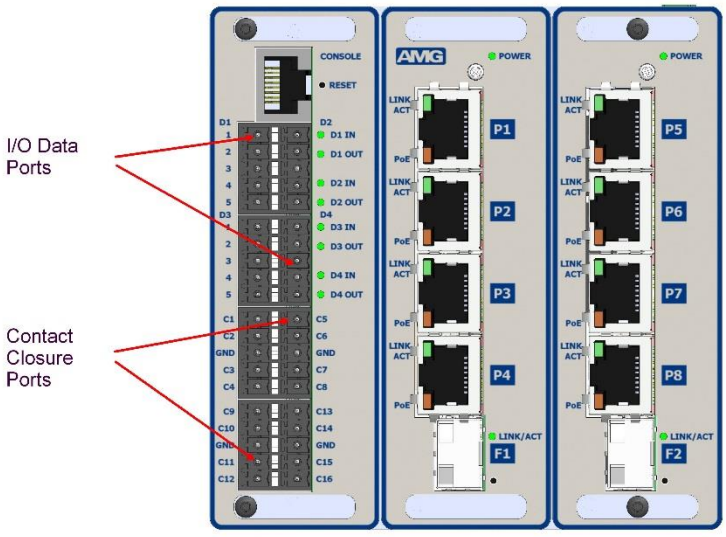


Figure 2-4 : I/O Connections

2.4 Pin Layout of I/O Connectors

Serial Data Ports D1-D4
Note: (A) or (B) in brackets in the tables below refer to RS-485 / RS-422 data specification

Data Port	Pin No.	RS-422	RS-485	RS-232
D1	1	D1 Data OUT- (B)	D1 Data IN/OUT- (B)	D1 Data OUT (Tx)
D1	2	D1 Data OUT+ (A)	D1 Data IN/OUT+ (A)	
D1	3	GND	GND	GND
D1	4	D1 Data IN- (B)		
D1	5	D1 Data IN+ (A)		D1 Data IN (Rx)

Data Port	Pin No.	RS-422	RS-485	RS-232
D2	1	D2 Data OUT- (B)	D2 Data IN/OUT- (B)	D2 Data OUT (Tx)
D2	2	D2 Data OUT+ (A)	D2 Data IN/OUT+ (A)	
D2	3	GND	GND	GND
D2	4	D2 Data IN- (B)		
D2	5	D2 Data IN+ (A)		D2 Data IN (Rx)

Data Port	Pin No.	RS-422	RS-485	RS-232
D3	1	D3 Data OUT- (B)	D3 Data IN/OUT- (B)	D3 Data OUT (Tx)
D3	2	D3 Data OUT+ (A)	D3 Data IN/OUT+ (A)	
D3	3	GND	GND	GND
D3	4	D3 Data IN- (B)		
D3	5	D3 Data IN+ (A)		D3 Data IN (Rx)

Data Port	Pin No.	RS-422	RS-485	RS-232
D4	1	D4 Data OUT- (B)	D4 Data IN/OUT- (B)	D4 Data OUT (Tx)
D4	2	D4 Data OUT+ (A)	D4 Data IN/OUT+ (A)	
D4	3	GND	GND	GND
D4	4	D4 Data IN- (B)		
D4	5	D4 Data IN+ (A)		D4 Data IN (Rx)

Table 2-5 : Serial Data I/O Connections

Contact Closure ports C1-C16

The AMG 9IM2x/9HM2x provides 16 contact closure inputs / outputs. Each contact closure may be configured as either an input (IN) or an output (OUT).

Each CC IN is a digital ON/OFF input typically used to detect contact closure status. The detection circuit is via an internal 8.2kΩ series resistor with a 47kΩ pull-up resistor to the internal +3V3 supply.

LOW level : input voltage < 0.5V or a low impedance (0Ω to 1kΩ) short circuit to GND
HIGH level : input voltage > +3V3 to +24Vdc or an open circuit.

Each CC OUT is a digital ON/OFF output (current sink) typically used to convey contact closure status. Each output circuit is an open drain power MOSFET with series 4.7Ω resistor and has a maximum rated continuous load current of 250mA, and maximum input voltage of +24Vdc.

Pin name	Pin name
C1	C5
C2	C6
GND	GND
C3	C7
C4	C8
C9	C13
C10	C14
GND	GND
C11	C15
C12	C16

Table 2-6 : Contact Closure I/O Connections

2.5 Power Connector

The number of Power Connectors and the type of PSU used in AMG 9IM2x/9HM2x depends on the device variant and whether Power over Ethernet (POE) is supported on the device. The supply voltage is :

- +48V DC to +56V DC – For POE variant.
- +12V DC to +24V DC – For non-POE variant.

☞ Please note : If the total system load exceeds 240W, additional Power Connectors will be fitted to enable power distribution from one or more PSU.

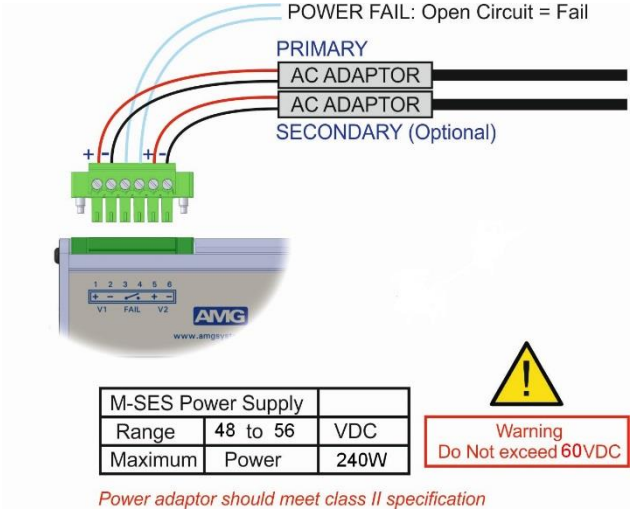


Figure 2-5 : PoE Power Connections

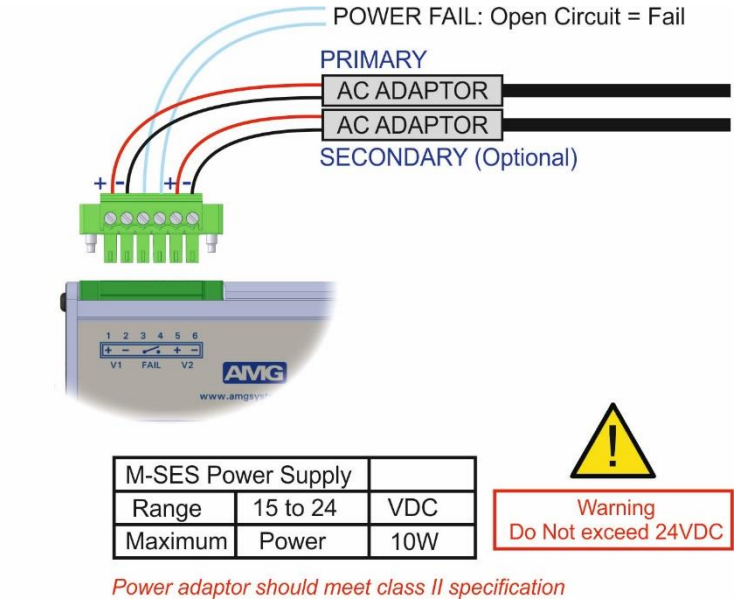


Figure 2-6 : Non PoE Power Connections

2.6 Power over Ethernet

Power over Ethernet (PoE) is a provision to power over Ethernet cables. So, an Ethernet cables carries both data and current together to operate devices like IP cameras. This is very helpful to install devices in remote places such

as ceilings, where it is hard to find power outlets. Only smaller devices can be powered using the PoE, as it carries limited power over the Ethernet.

1. The original IEEE 802.3af-2003 PoE standard provides up to 15.4 W of DC power (minimum 44 V DC and 350 mA) to each device. Only 12.95 W is assured to be available at the powered device as some power is dissipated in the cable.

2. The updated IEEE 802.3at-2009 PoE standard also known as PoE+ or PoE plus, provides up to 25.5 W of power per port/device.

3. PoE-U / PoH non-ratified standards provide up to 60W / 90W of power per port/device.

Here are POE specifications of **AMG 9IM2x/9HM2x** per port :

Parameter	PoE	PoE+	PoE-U	PoH
Input Voltage	48-50V	56-60V	56-60V	56-60V
Output Power	15W	25W	60W	90W
Output Voltage	44-48V	52-56V	52-56V	52-56V

Table 2-7 : POE Specifications

☞ Please note : System load should not exceed 240W on each Power Connector.

2.7 Ethernet Port LEDs

Each non-transceiver Ethernet port has two LEDs - Link/Activity and PoE power output status. These are are situated on the left side of each RJ45 port-connector as depicted below:

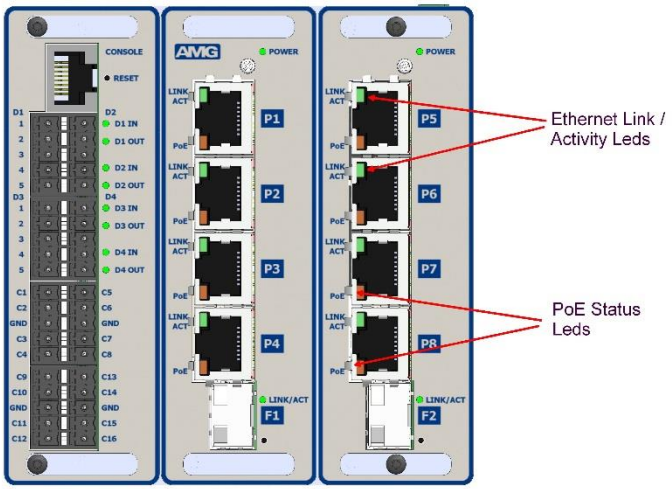


Figure 2-7 : Ethernet Port LEDs

Each SFP Ethernet transceiver port has a single LED - Link/Activity. This is situated on the right side of each SFP port-connector as depicted below:

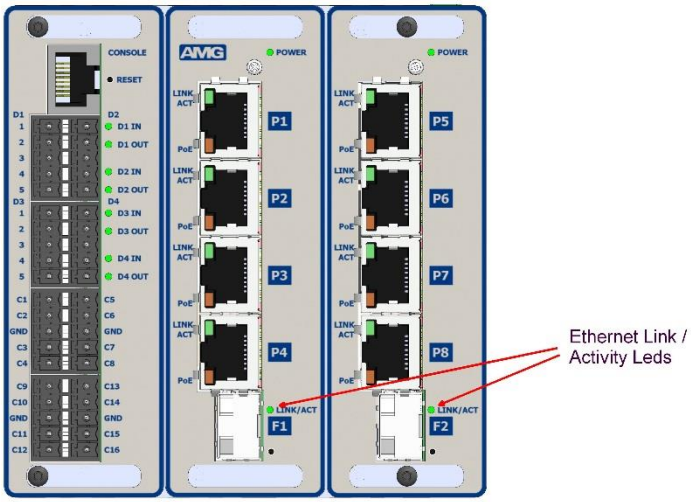


Figure 2-8 : SFP Transceiver Port LEDs

2.8 I/O Port LEDs

I/O port LEDs may be present on the front panel depending on the variant of the **AMG 9IM2x/9HM2x**.

Models which support serial data ports, contact closure signals /alarm have LED indicators to display the status on the input/output. These LEDs are depicted as follows:

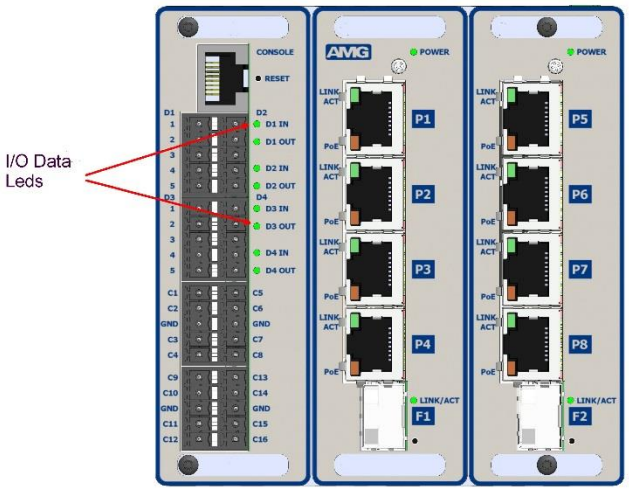


Figure 2-9 : I/O Port LEDs

Chapter 3

HS-IO Hardware Description

This section describes **HS-IO** hardware. It describes how different ports, LEDs and connectors are to be used.

In order to provide very low latency (< 5 milliseconds) end to end transmission of serial data over IP, the AMG M-SES can be equipped with a “high-speed” / low latency serial data expander module which provides 2 or 4 bi-directional serial data ports which are individually configurable for RS-232 / RS-485 or RS-422 serial data:

AMG9HMX-2S : 2 serial data ports.
AMG9HMX-4S : 4 serial data ports.

Future options will also provide contact closure variants as follows:

AMG9HMX-2S8C : 2 serial data ports, 8 Contact Closures.
AMG9HMX-4S4C : 4 serial data ports, 4 Contact Closures.

Use the following hyperlinks to view the various hardware features:

3.1 HS-IO Connections

☞ Note : The Expander Module is connected to the M-SES unit by an external Ethernet (100Mbps) RJ45 to RJ45 Patch cable.

Power Connection

Connector Type……Removable 2-pin, 3.81mm, Screw Terminal
Connector Partno……Phoenix 1803578
Supply Voltage……+12 to +15 Volts DC
Maximum Power……..1 Watt

Data and Alarm Channel Connections

No. of Data Channels……..2 or 4
No. of Alarms……...4 or 8

Connectors……Removable 5-pin, 3.5mm, Spring Terminal
Connector Partnos……Phoenix 1952296

Data Interfaces……..RS-232 / 422 / 485. Selected by external slide switches D1-D2

RS-232 – Switch Position - Top

RS-422 – Switch Position - Middle

RS-485 – Switch Position - Bottom

Internal 120Ω termination resistors may be applied to RS-422 or RS-485 inputs as required by internal DIL switches (P0-P3) inside the enclosure. The switches may be accessed by removing the 2 fixing screws in the rear panel and sliding the PCB out of the enclosure.

Alarm inputs……..Input is via a series 10k resister with 47kΩ pull-up to +3V3.
Alarm outputs……Output is NPN open collector, maximum load 500mA @ 24Vdc

Ethernet Connection

Ethernet Data Connector…….....RJ45
Interface……Auto-negotiation up to 100BASE-TX full duplex
Ethernet Data Rate……..100Mb/s.

3.2 HS-IO Front panel LEDs

Power LED

Power……	Green	-	Unit powered.

Low Speed Data LEDs

Data Present IN (RS-485 or RS-422)…..Red		-	data present on IN+, IN-
	Off	-	data not present on IN+, IN-
Data Present IN (RS-232)……..Green		-	logic zero (+V) present on input IN+
	Red	-	logic transitions present on IN+
	Off	-	logic one (-V) present on input IN+

IN corresponds to the data signals being transmitted onto network

Data Present OUT (RS-485 or RS-422)..Red		-	data present on OUT+, OUT-
	Off	-	tristate / data off on OUT+, OUT-
Data Present OUT (RS-232)……..Green		-	logic zero (+V) present on OUT+
	Red	-	logic transitions present on OUT+
	Off	-	logic one (-V) present on OUT+

OUT corresponds to the data signals being received from network

Contact Closure LEDs

Channels 1-8

ALARM IN……Green		-	Contacts closed.
	Off	-	Contacts open.
ALARM OUT……...Green		-	Contacts closed.
	Off	-	Contacts open.

Ethernet Data LEDs

Link not Present……Yellow		-	Link not present
	Off	-	Link is present
Link Integrity……Green		-	Link integrity is good, Idle state
	Green Blink	-	Data transfer
	Off	-	Link not present

Data Channel and Contact Closure Configuration

The 4 physical serial data interfaces RS-485, RS-422 or RS-232 are individually selectable by the user with the slide switches mounted on the rear panel.

There are also 2 or 4 bi-directional Contact Closure inputs/outputs. Each contact closure can receive an on/off signal and is typically used to convey contact closure status.

3.3 HS-IO Data Channel Interface

Each low speed data channel provides an RS-232, RS-422 (full duplex, four wire) or RS-485 (half duplex, two wire) interface defined by the slide switch mounted from the rear panel Every data channel as shipped from the factory is set up for RS-485 operation unless otherwise requested.

The OUT+- data drivers for RS-485 and RS-422 modes will be in the OFF (tristate condition) unless OUT data is being transmitted.

HS-IO Data Interface Connections

Connector Pin No.	Data Channel		
	RS-485 [switch bottom]	RS-422 [switch middle]	RS-232 [switch top]
1	IN/OUT - (B)	OUT - (B)	OUT
2	IN/OUT + (A)	OUT + (A)	
3	GND	GND	GND
4		IN - (B)	
5		IN + (A)	IN

Table 3-1 : HS-IO HS-IO Serial Data Interface Connections

Note : (A) or (B) in brackets in the above table refers to RS-485 / RS-422 data specification.

HS-IO Data Channel Termination

The interface mode RS-232, RS-422 or RS-485 of each data port Data 1-4, is selected with the corresponding external slide switch D1-D4. The actual number of data channels provided on the unit depends upon the AMG model.

Internal 120Ω termination resistors across IN+ and IN- inputs may also be applied when in RS-422 or RS-485 mode using internal DIP switches P0-P3 on the main PCB inside the enclosure. P0-P3 may be accessed by removing the 2 fixing screws in the rear panel and sliding the PCB out of the enclosure.

For clarity, in the 3 examples shown below all 4 data ports D1-D4 are terminated the same, but each data channel may be configured & terminated independently as required. The 3 examples shown are RS-232 (no termination), RS-422 (120Ω) or RS-485 (120Ω).

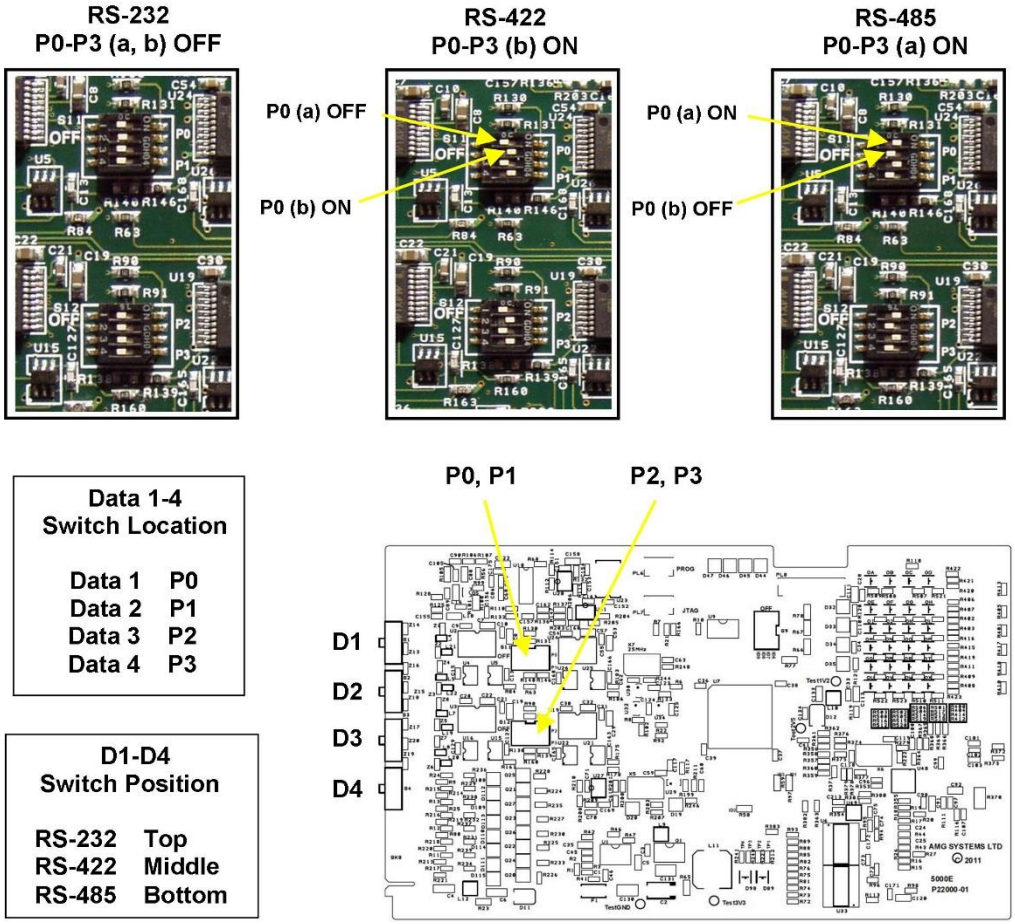


Figure 3-1 : HS-IO Serial Data Interface Connections

3.4 HS-IO Contact Closure Interface

High Speed Serial Expander also provides 4 or 8 bi-directional contact closure inputs/outputs.

Each CC IN input is via an internal 10kΩ series resistor with a 47kΩ pull-up resistor to the internal +3V3 supply.

Each CC OUT output is an NPN open collector circuit with a maximum rated continuous load of 500mA / 24Vdc.

HS-IO Contact Closure Connections

Connector Pin No.	Contact Closures	
	CC IN 1-4, 5-8	CC OUT 1-4 , 5-8
1	CC 1/5 IN	CC 1/5 OUT
2	CC 2/6 IN	CC 2/6 OUT
3	GND	GND
4	CC 3/7 IN	CC 3/7 OUT
5	CC 4/8 IN	CC 4/8 OUT

Table 3-2 : HS-IO HS-IO Contact Closure Connections

Chapter 4

Installation Guide

This section describes how to install the **AMG 9IM2x/9HM2x** Multi-Service Ethernet Switch.

Use the following hyperlinks to view the various installation features:

4.1 Unpacking the Switch

Before unpacking the switch, inspect the package and immediately report any evidence of damage.

i. Place the box on a clean flat surface.
ii. Open the box or remove the box top.
iii. Carefully remove the switch from the box and place it on a secure and clean surface.
iv. Remove all packing material.
v. Inspect the switch and accessories for damage. Report any damage immediately.

While unpacking the switch, ensure that the following items are included:

- Ethernet Switch
- AC power Adaptor & IEC Mains cable
- RS-232 console cable / RJ45 Adaptor
- Documentation CD
- Product Quick Start Guide

4.2 Installing Pre-requisites

AMG 9IM2x/9HM2x series devices can be mounted in a standard equipment rack or enclosure, using industry standard DIN rail. Before installing the unit, verify that the chosen location for installation meets the following site requirements:

Power: the unit is installed near an easily accessible 100-240 VAC, 50-60 Hz outlet.

Clearance: there is adequate frontal clearance for operator access. Allow clearance for cabling, power connections, and ventilation.

Cabling: the cabling is routed to avoid sources of electrical noise such as radio transmitters, broadcast amplifiers, power lines, and fluorescent lighting fixtures.

Ambient Requirements: the ambient unit operating temperature range is -20 to 74ºC at a relative humidity of 0% to 95%, non-condensing.

4.3 Mounting the Switch

Mounting the unit is shown as follows:

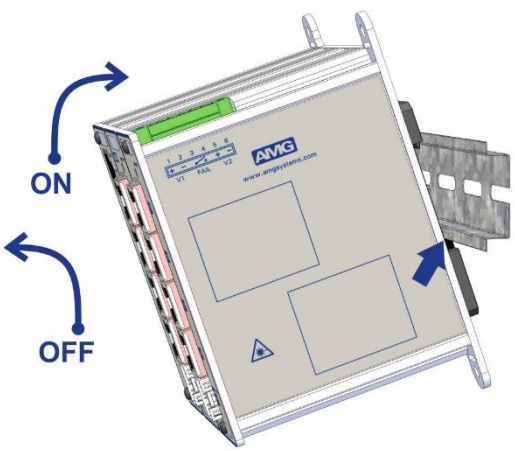


Figure 4-1 : Mounting the unit - DIN Rail

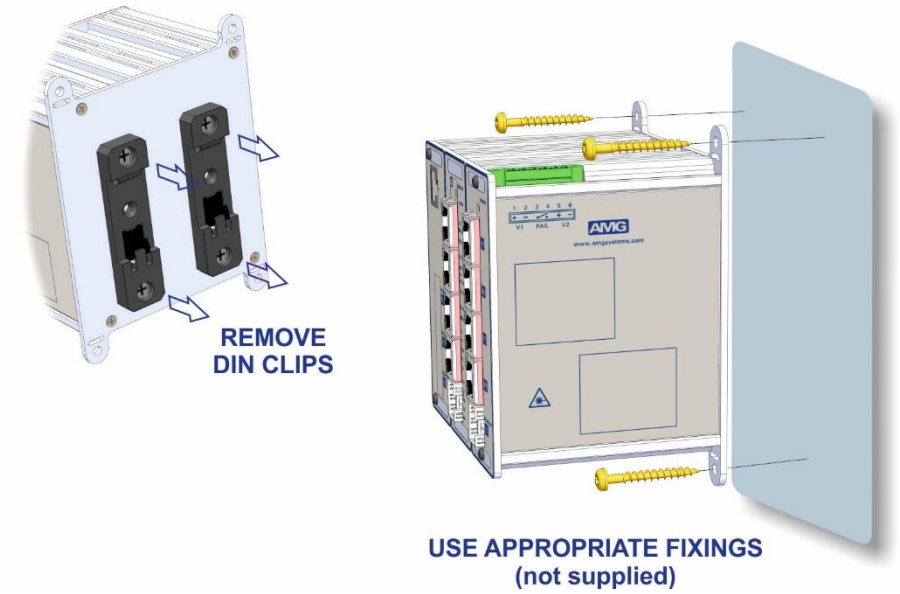


Figure 4-2 : Mounting the unit - Surface

4.4 Power Connections

Plug the supplied IEC-8 mains power cable to the AC adaptor mains input connector.

Plug the AC adaptor DC output connector into the DC power input connector on the AMG 9IM2x/9HM2x switch top panel.

Turn the incoming mains supply on and confirm that the switch is receiving power and operating correctly by examining the LEDs on the front panel.

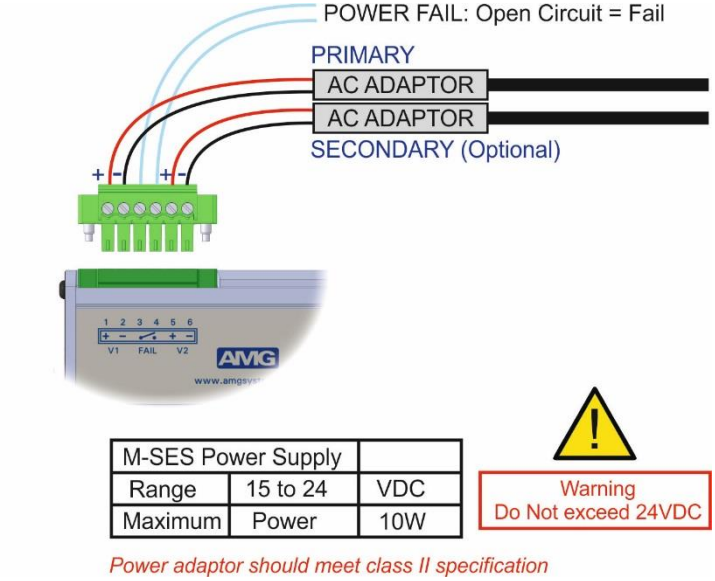


Figure 4-3 : DC Power Connection

4.5 Connecting to Network

Configuration, Management and maintenance of AMG 9IM2x/9HM2x switch is done through web management interface. In order to operate switch, it should be have IP for connectivity. Switch can get can IP either through DHCP or through static IP address assignment.

If the switch is assigned a non-default static IP address, it is labelled on the side panel of the switch. Otherwise, switch operates at a static IP address – 192.168.1.101

Connecting the switch with default IP address can be depicted as follows:

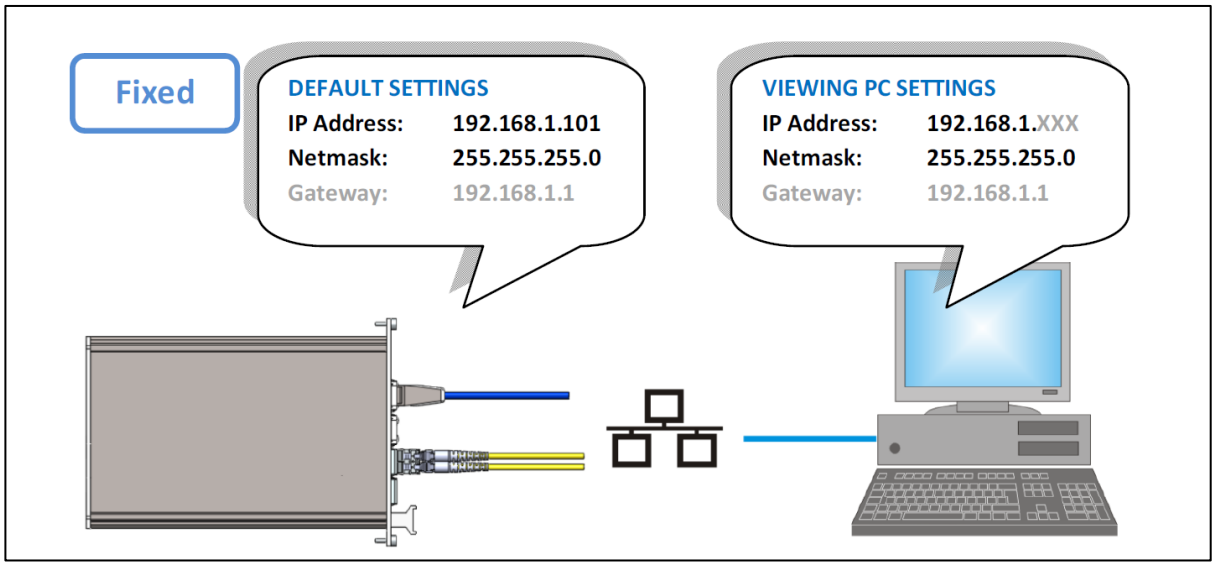


Figure 4-4 : Network Connections

4.6 Connecting to RS-232 Management Console

If access to AMG 9IM2x/9HM2x switch via CLI (Command Line) interface is required, connect the **Console** cable / adaptor RJ45 into the console port and connect the DB9 serial RS-232 data port to a PC or similar.

RS232 Connections

Console	TX-Out	RX-In	Gnd	No Connection
RJ45	2	3	5	1,4,6,7,8
DB9	2	3	5	1,4,6,7,8,9

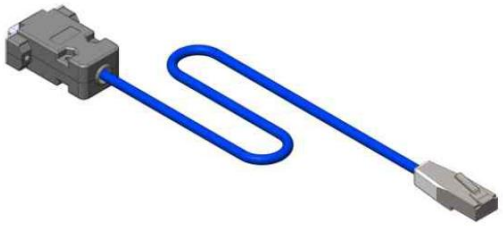


Figure 4-5 : Console Connections

Login to the AMG 9IM2x/9HM2x switch via CLI (Command Line) interface

Connect using a terminal application such as PuTTY or RealTerm : Serial COM port, Speed 115200

Default logon "**Admin**" Password "**Admin**"

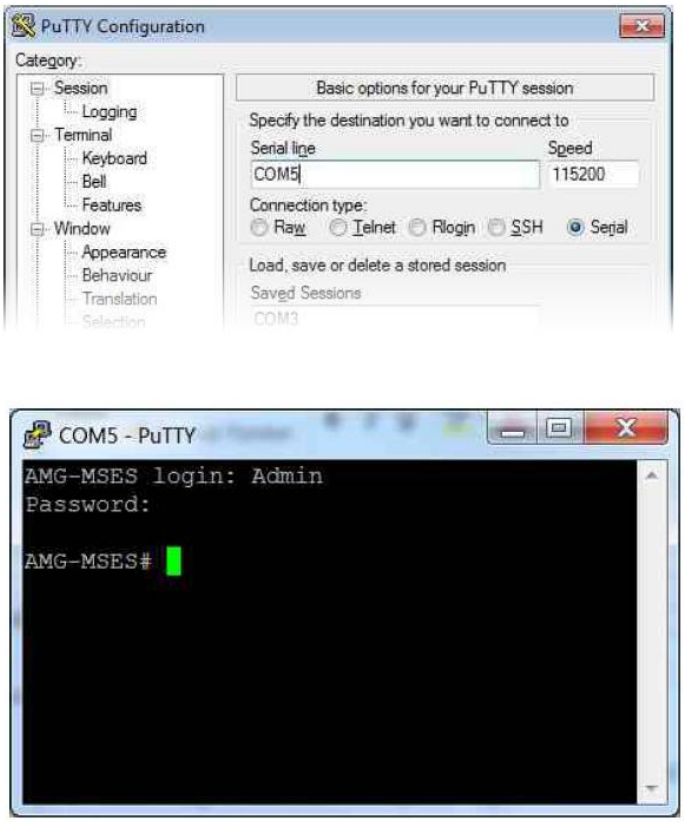


Figure 4-6 : Login through CLI

Chapter 5

Web Interface Conventions

This section describes how the Web Interface is used to view, configure and control the **AMG 9IM2x/9HM2x** Multi-Service Ethernet switch.

Use the following hyperlinks to view the various Web Interface features:

5.1 WEB interface

AMG 9IM2x/9HM2x WEB interface is composed of different screen elements which are used to get input from user and/or to display output. These screen elements are Text Fields, Number Fields, Option Buttons, Check Boxes, Combo Boxes, Buttons, Text Areas and Lists.

Web User Interface facilitates new and inexperienced users to create the basic routing and security functions, quickly and effectively.

Note : some advanced configuration options can be set only through the CLI.

A field entry with a * symbol displayed in a Web screen, denotes that it is a mandatory field.

The following sample screens depict the **AMG 9IM2x/9HM2x** Web interface with the standard screen elements named, as it is used in this document.

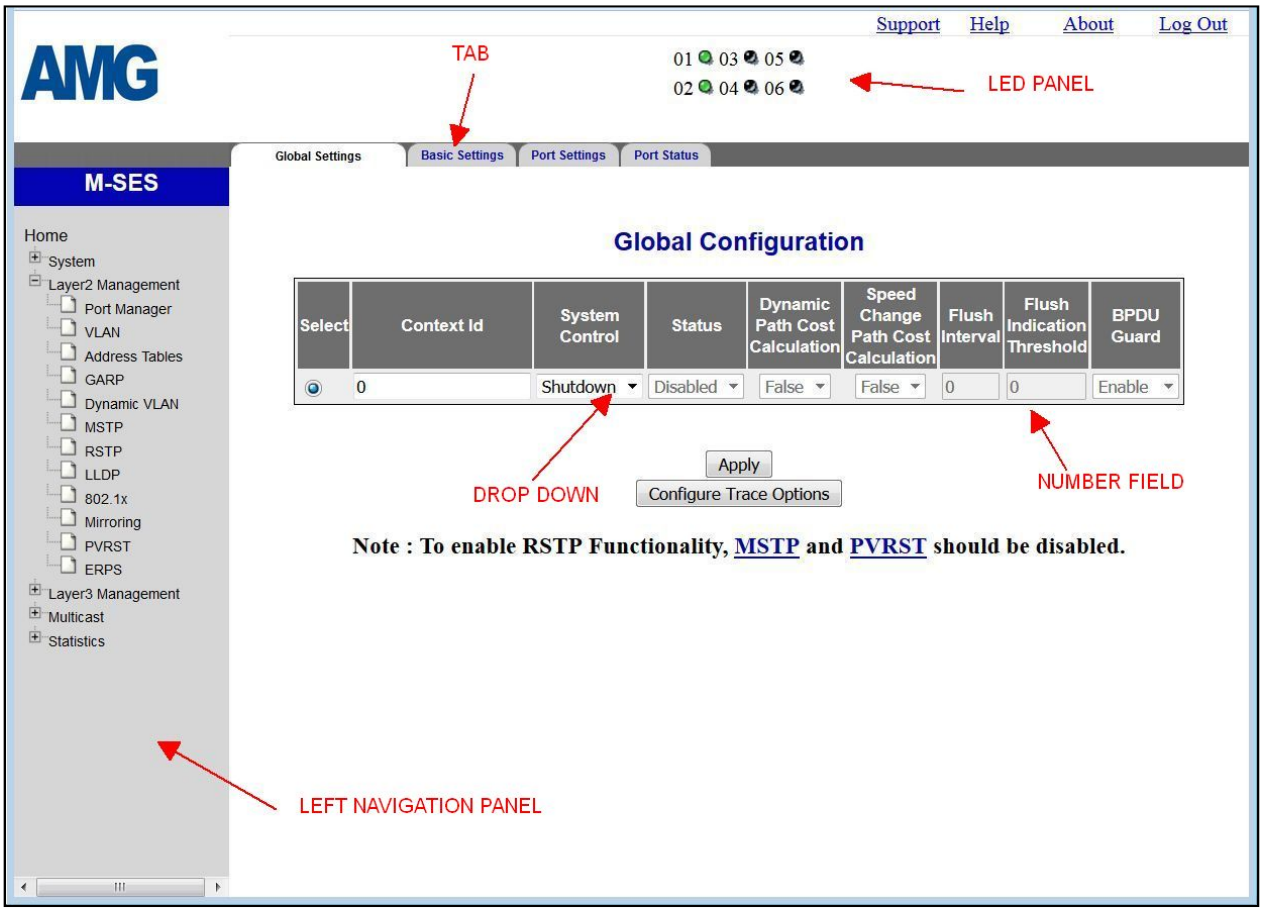


Figure 5-1 : Web GUI screen sample 1

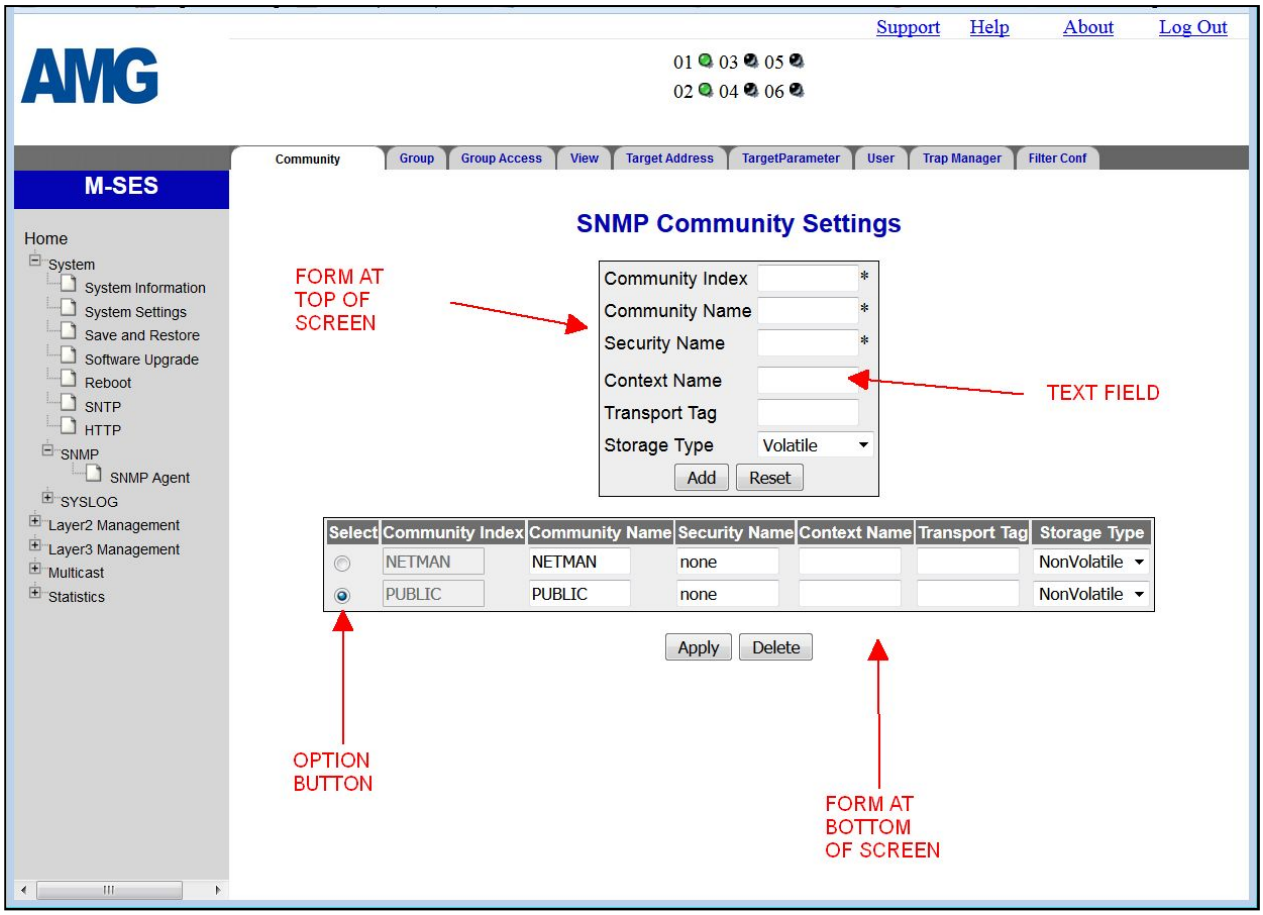


Figure 5-2 : Web GUI screen sample 2

5.2 Internet Explorer Settings

For Product screens viewed in Internet Explorer, ensure the browser setting is as given below;

Click **Tools** from the Menu bar of the browser.

Figure 5-3 : Browser General Settings Tab

Under General tab, click on **Browsing History Settings**.

Figure 5-4 : Browser History Settings

Select "**Every time I visit the webpage**" option as shown.

Click **OK**.

5.3 Document Conventions

Definitions and Acronyms**Error! Reference source not found.** lists the erms and typographical conventions used in this document.

Convention	Usage	Example
Arial Bold 10	**Navigation** path to each screen. Includes tab name also.	**System > IP Authorized Manager > IP Authorized Manager**.
	Any references to screen elements like action **Buttons**, option **Buttons**, check boxes, screens names.	There are two options to save the configuration data namely, **Flash Save** and **Remote Save**.
Arial 10 Italics	User Inputs to **Fields**	Specify the name of the configuration file available in the remote system. The default file name is *AMG.conf*.
	Denotes any additional information on an associated topic.	All the configurations are active only when the SNTP module is enabled.

Table 5-1 : Conventions Used in this Document

Chapter 6

Logging into AMG 9IM2x/9HM2x

The **AMG 9IM2x/9HM2x** WEB User interface allows the user to control various parameters at the System Level and Protocol level.

The basic configurations such as provisioning of default IP address, VLAN configuration etc. may also be performed through the console CLI (Command Line Interface) provided by AMG 9IM2x/9HM2x .

Use the following hyperlinks to view the various Logging into the switch features :

- Login
- Home Screen

6.1 Login

Launch a web browser compatible with AMG 9IM2x/9HM2x on your PC. Enter the Switch IP address in the Address bar of the web screen. For example, if the IP address of the Switch interface is 192.168.1.101, then enter **http://192.168.1.101** in the address bar of the Web browser to access the Switch

AMG 9IM2x/9HM2x is compatible with Internet Explorer 11.0, Mozilla Firefox 40 and above

The screenshots depicted in this document are configured with Firefox.

Figure 6-1 : Login Screen

Screen Objective	This screen allows the user access **AMG 9IM2x/9HM2x** through WEB User Interface
Fields	• **UserName** - Enter the username.The default username is **Admin**. • **Password** - Enter the password. The default password is **Admin**. This user name and password are set by default in the Switch. The Command Line Interface can be used to create new users, delete existing users and modify own password or the password of other existing users. Refer the CLI user manual for details.

The maximum login attempts with wrong password is by default set as 3. This can be configured through CLI. The maximum login attempts value ranges from 1 to 10.

Buttons	• **Login** - To login to AMG 9IM2x/9HM2x and view the **AMG 9IM2x/9HM2x Home** screen.

6.2 Home Screen

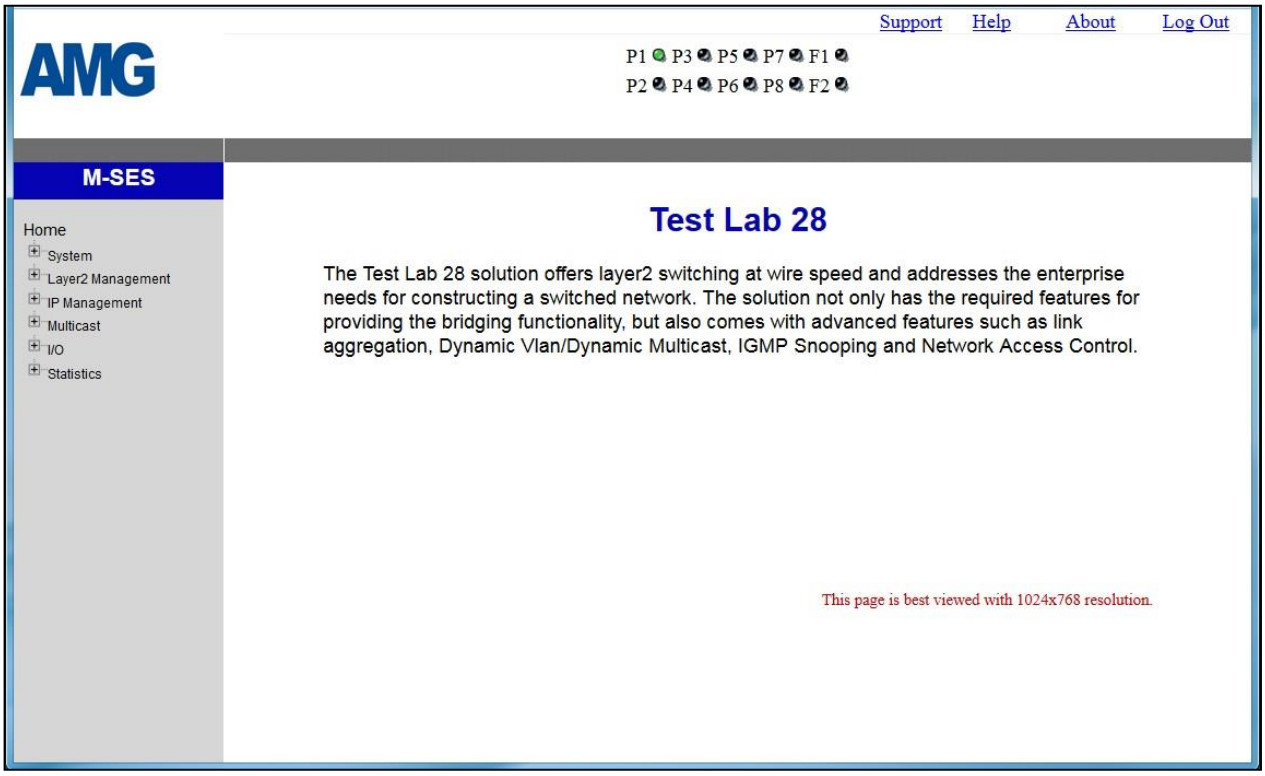


Figure 6-2 : Home Screen

Screen Objective	This screen provides the user basic information about AMG 9IM2x/9HM2x and also provides links to configure system and protocol parameters.

The Switch name shown on this screen and some other screens is set by the user on System Information Page. In the screenshot above it is "Test Lab 28"

Navigation	On successful Login from the **Login** screen.
Links	• **Left Navigation Pane** - Links to Management screens to access system and protocol configuration screens. The links are categorized based on the protocol feature and functionality:

- **Right Top corner Links** - The following standard set of links is displayed on the right hand side top corner of the all the Web screens:
  - Support: To get high-quality and responsive technical support.
  - Help: To open the help screen.

    Help text is currently not available.
  - About: To get additional information about Web management.
  - Log Out: To Log out the Web session through which the user is connected.

Chapter 7

Left Navigation Pane

This chapter describes the organization of the sub-menus and features available from the Left Navigation Pane.

The **System and Management** parameters are configured through the screens displayed by the following items in the Left Navigation Pane :

- System
- Layer2 Management
- IP Management
- Multicast
- I/O Management
- Statistics

7.1 System

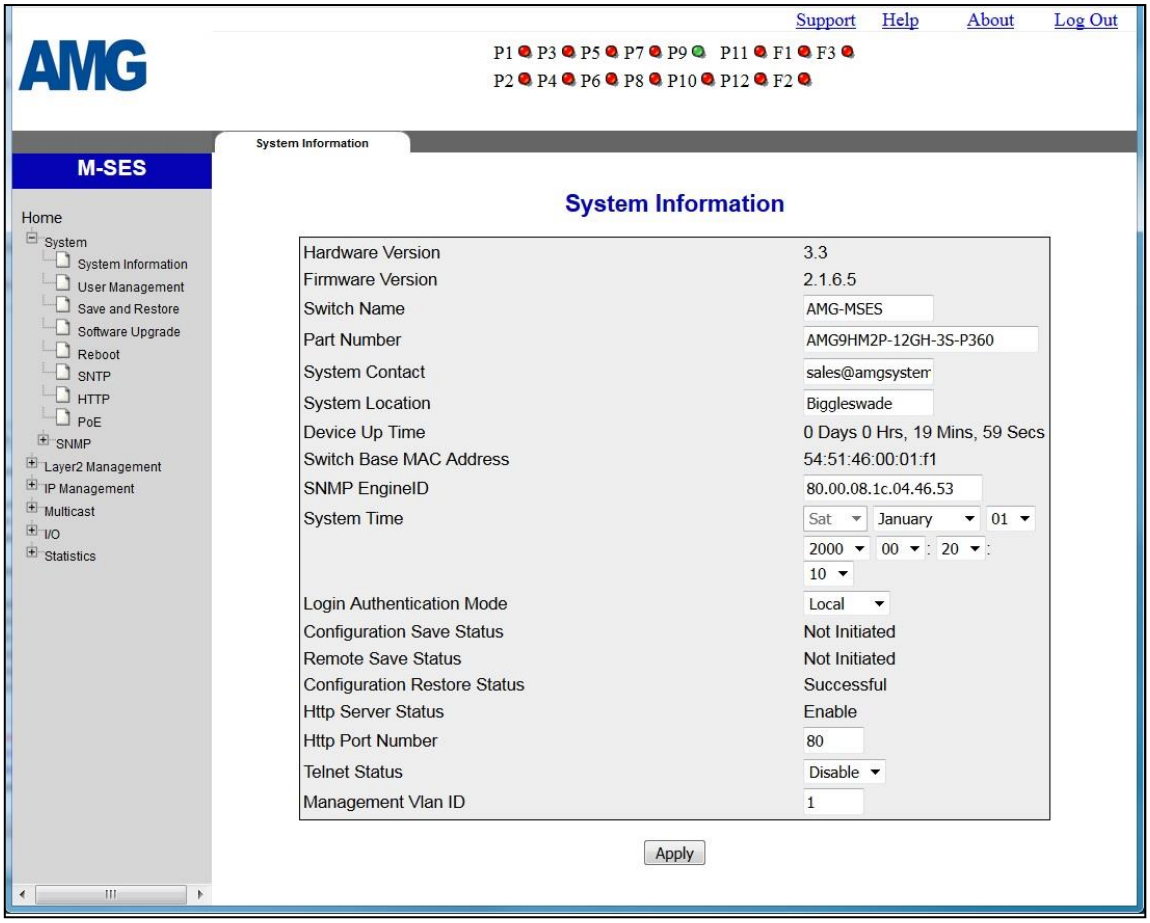


Figure 7-1 : System Information Home Page

This link has sub-links in the left navigation pane for all system specific configurations and system specific modules. You can perform system specific configurations through the screens displayed by these links.

The **System** link on the left pane provides access to the following links. These are included as individual chapters in the user manual.

- System Information
- User Management
- Save and Restore
- Software Upgrade
- Reboot
- SNTP
- HTTP
- PoE
- SNMP

7.2 Layer2 Management

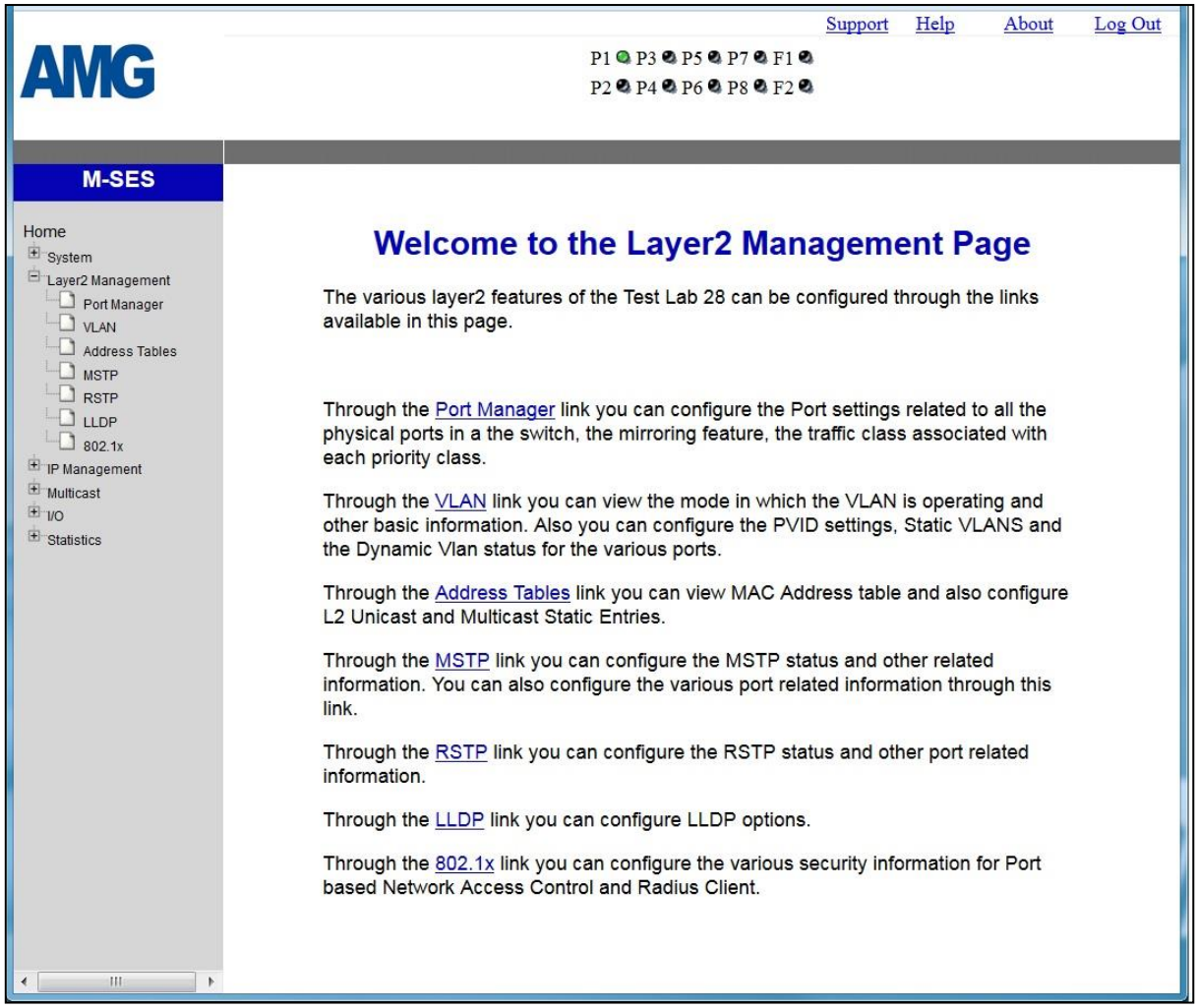


Figure 7-2 : Layer2 Management Home Page

This link has sub-links for all Layer2 related features and modules. You can perform Layer2 configurations through the screens displayed by these links.

The **Layer2 Management** link on the left pane provides access to the following links. These are included as individual chapters in the user manual.

- Port Manager
- VLAN
- Address Tables
- MSTP
- RSTP
- LLDP
- 802.1x

7.3 IP Management

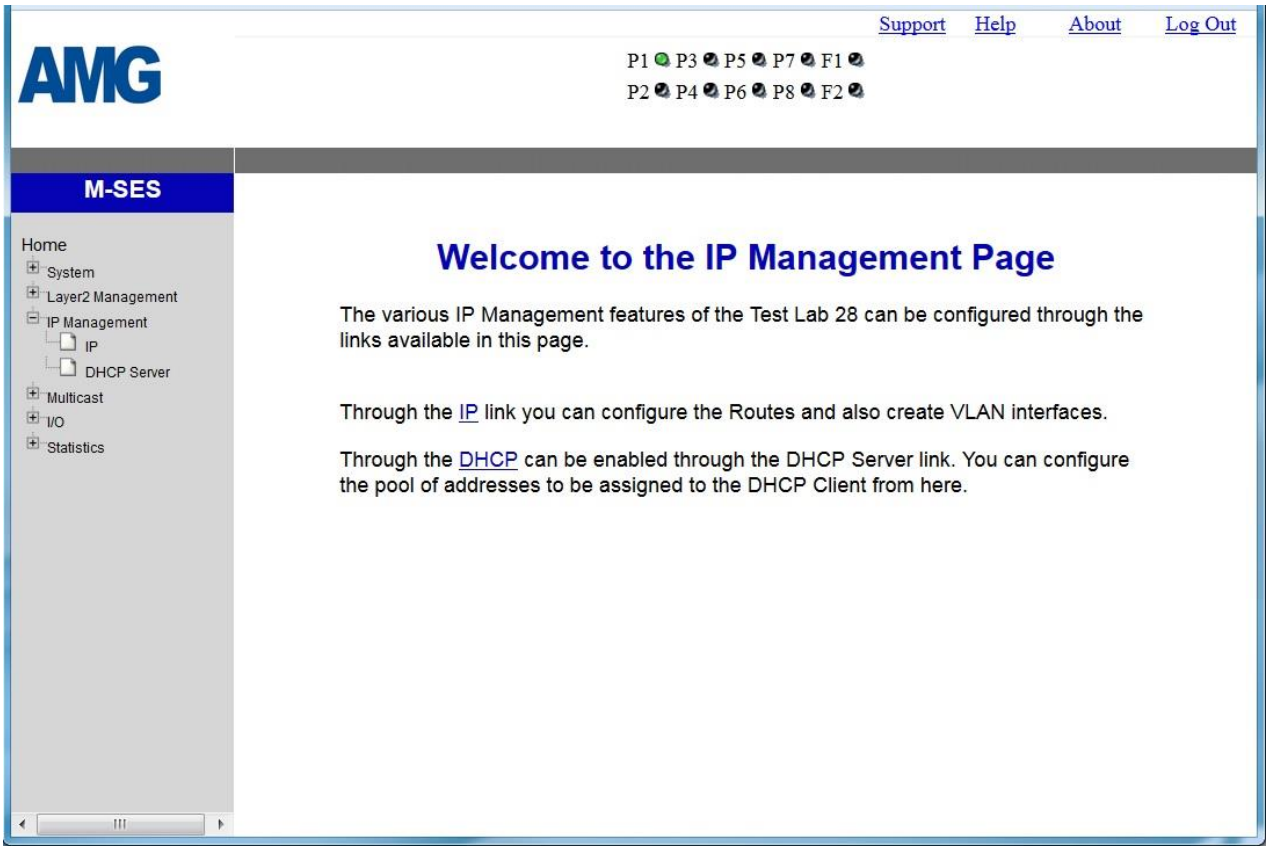


Figure 7-3 : IP Management Home Page

This link has sub-links for all IP related features and modules. You can perform IP configurations through the screens displayed by these links.

The **IP Management** link on the left pane provides access to the following links.

- IP
- DHCP Server

7.4 Multicast

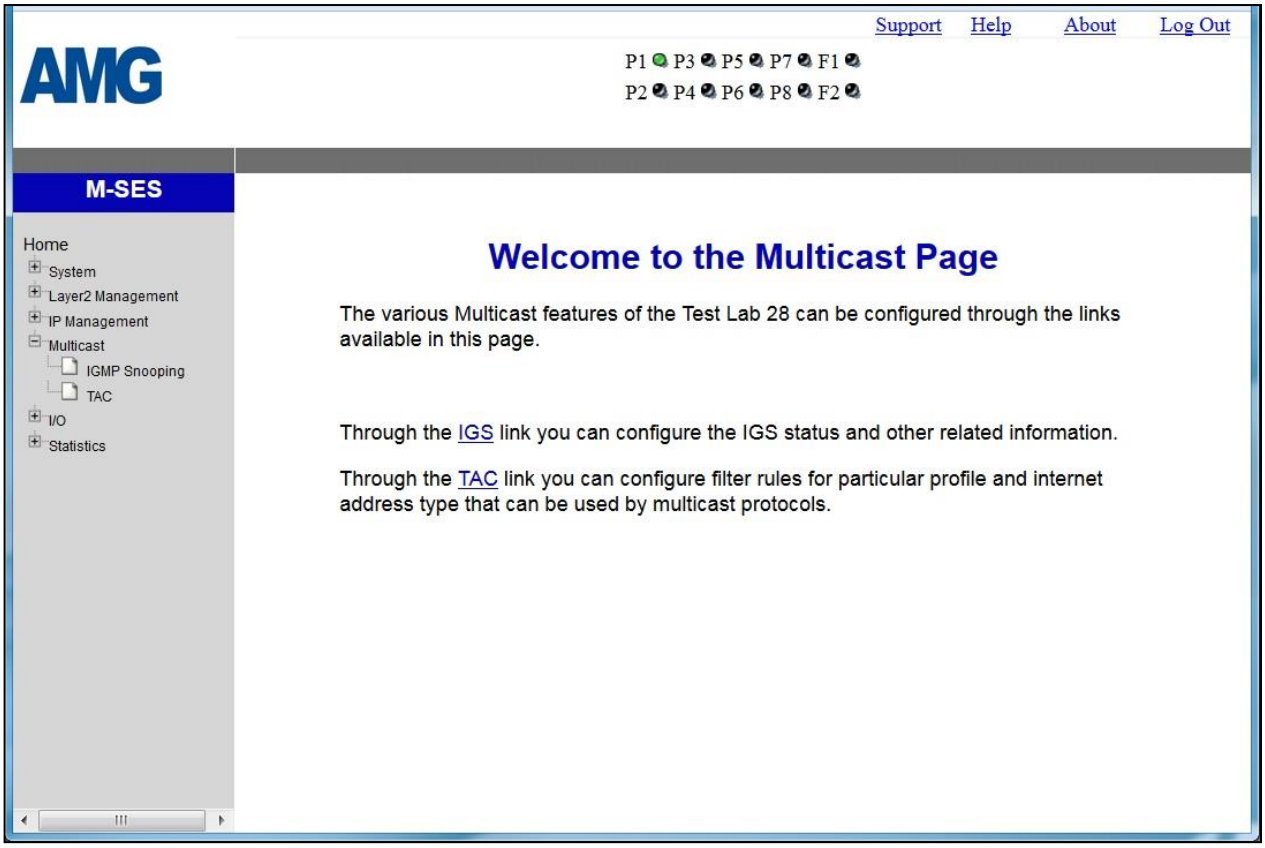


Figure 7-4 : Multicast Home Page

This link has sub-links for multicast protocols, which are involved in transmitting a message to a set of selected multiple recipients.

The **Multicast** link on the left pane provides access to the following links.

These are included as individual chapters in the user manual.

- IGMP Snooping
- TAC

7.5 I/O Management

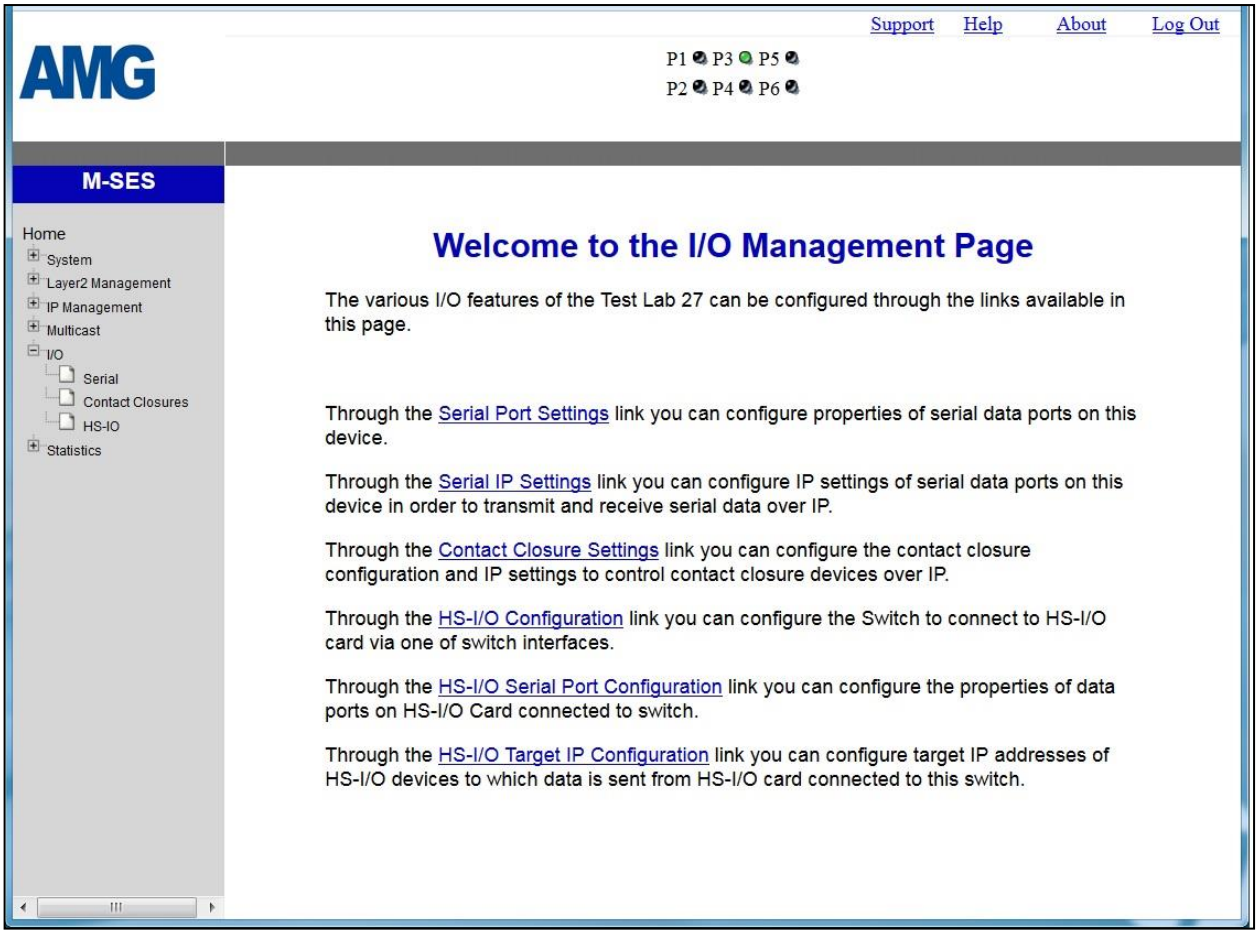


Figure 7-5 : I/O Management Home Page

This link has sub-links in the left navigation pane for all I/O specific configurations and system specific modules. You can perform I/O specific configurations through the screens displayed by these links.

The **I/O** link on the left pane provides access to the following links. These are included as individual chapters in the user manual.

- Serial
- Contact Closures
- HS-IO

7.6 Statistics

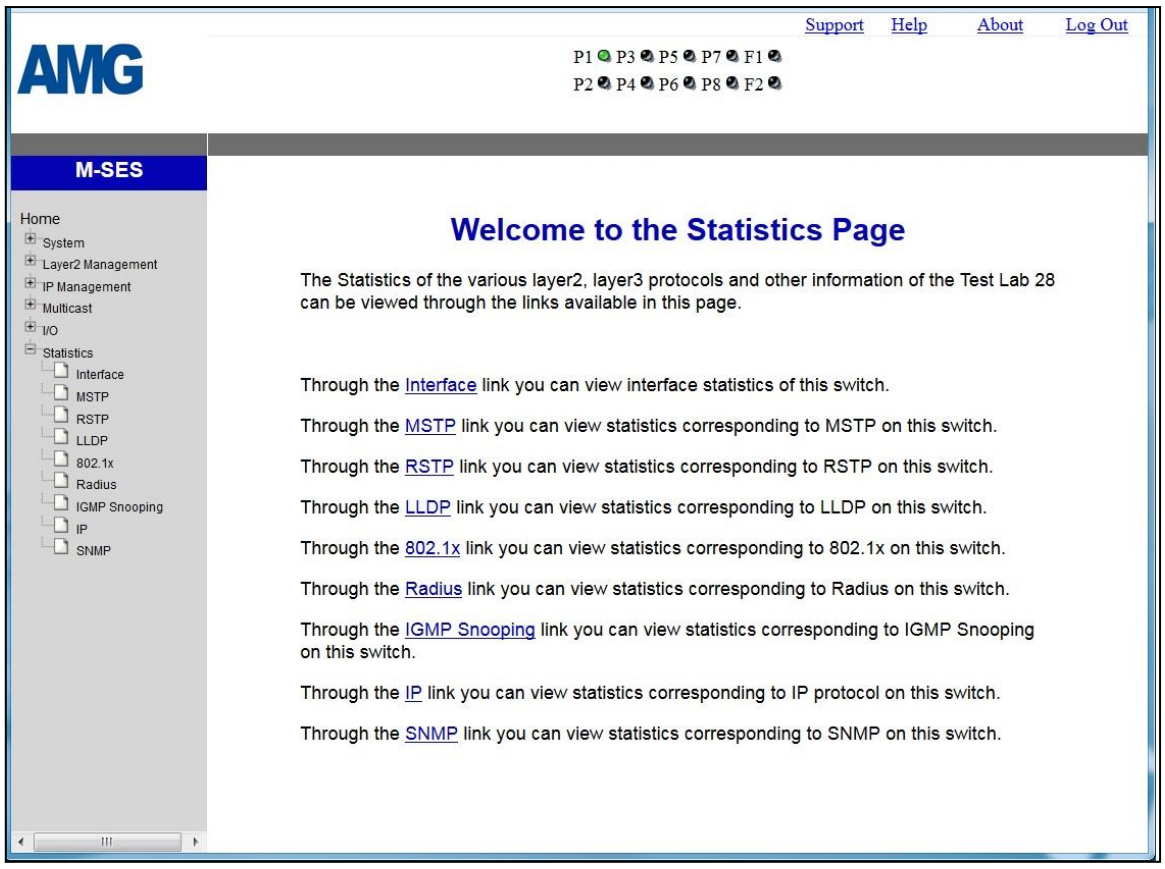


Figure 7-6 : Statistics Home Page

This link has sub-links for statistics of several modules and features. You can view statistics details.

The **Statistics** link on the left pane provides access to the following links. These are included as individual chapters in the user manual. Interface

- Interface
- MSTP
- RSTP
- LLDP
- 802.1x
- Radius
- IGMP Snooping
- IP
- SNMP

Chapter 8

System Information

To access System Information screens, click **System > System Information**.

8.1 System Information

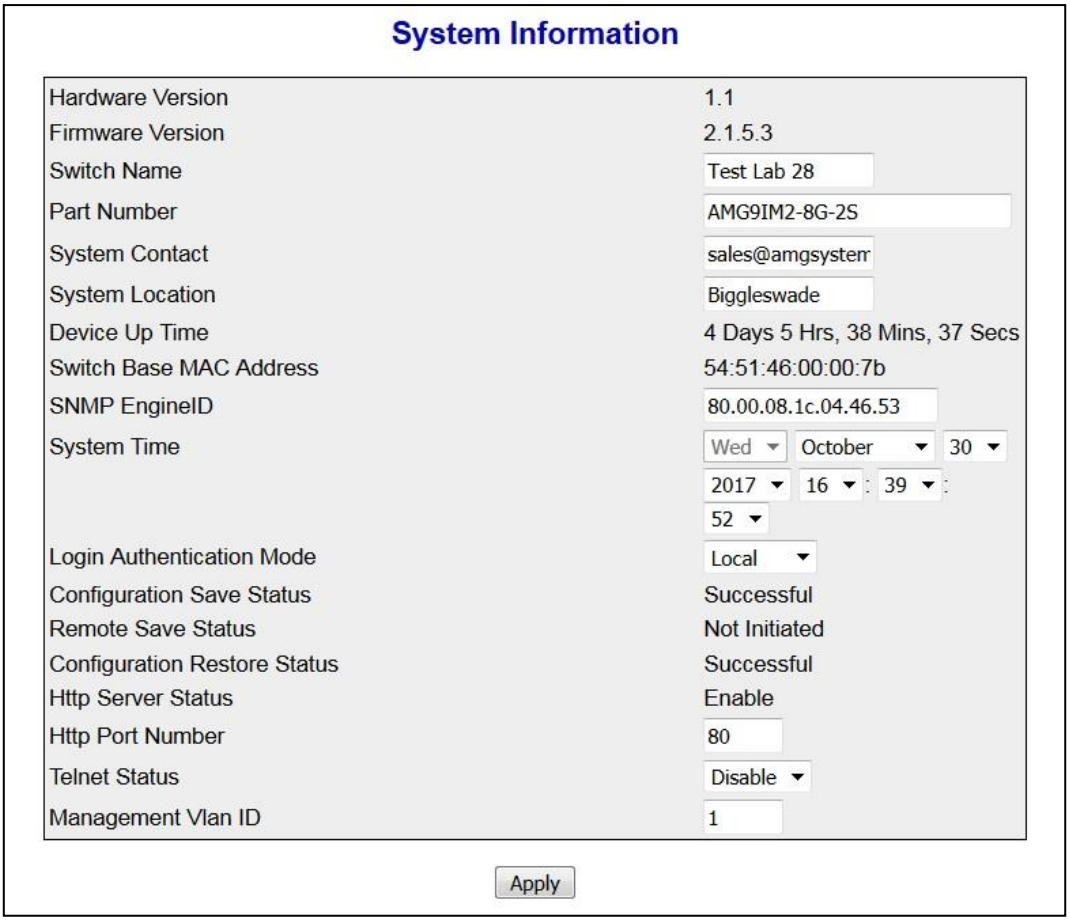


Figure 8-1 : System Information

Screen Objective	This screen allows the user to configure the system information
Navigation	**System > System Information**
Fields	• **Hardware Version** - Displays the hardware version number of the system. • **Firmware Version** - Displays the firmware version number of the system. • **Switch Name** - Enter the name for identifying the device. This value range is a string of size **15**. • **Part Number** - Displays the AMG Part number. • **System Contact** - Enter the contact person details for this managed node. This value range is a string of size **50**. If the contact information is not available, this value takes a zero-length string.

- **System Location** - Enter the physical location of this node. This value range is a string of size **50**.. If the location is unknown, this value takes a zero-length string.
- **Device Up Time** - Displays the time from which the device is up. The format is Days Hours, Minutes, Seconds Example: 0 Days 1 Hrs, 15 Mins, 27 Secs.
- **Switch Base MAC Address** - Displays the device's unique physical MAC Address in hexadecimal format i.e. 54:51:46:00:00:7b .
- **SNMP Engine ID** - Displays the device's unique identifier in hexadecimal format i.e. 80.00.08.1c.04.46.53.
- **System Time** - Select the current date and time The format is Day Month Date Year Hours Minutes Seconds Example: Fri May 07 2010 13: 40: 00. This value range is a string of size **40.**
- **Login Authentication Mode** - Select the login authentication mode. The list contains:
  - **Local** – Sets the authentication mode as Local. The user identification, authentication, and authorization method is chosen by the local system administration and does not necessarily comply with any other profiles.
  - **Remote** – Sets the authentication mode as Remote. Authentication is done in the remote location through a RADIUS (Remote Authentication Dial-In User Service) or TACACS server. RADIUS is a protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. TACACS (Terminal Access Controller Access-Control System) is a remote authentication protocol that is used to communicate with an authentication server commonly used in networks.
  - **Tacacs** - Sets the authentication mode as TACACS. Authentication is done through a TACACS+ server.
- **Configuration Save Status** - Displays the configuration save status. The default option is **Not Initiated** Once the configuration is done, the save status will be displayed as any of the following:
  - **Successful** – System information is configured and saved successfully.
  - **Failure** - System information configuration save failed.
  - **Inprogress** - System information configuration save is in-progress.
  - **Not Initiated** - System information configuration save is not initiated.
- **Remote Save Status** - Displays the remote save status. The default option is **Not Initiated** This status represents the status of save operation to the remote location as any of the following:
  - **Successful** –Remote information is configured and saved successfully
  - **Failure** - Remote information configuration save failed.
  - **In Progress** - Remote information configuration save is in-progress.

- **Not Initiated** - Remote information configuration save is not initiated.

- **Configuration Restore Status** - Displays the configuration restoration status. The default option is **Not Initiated** The already configured parameter will be restored and the status will be displayed as any of the following
  - **Successful** – Configuration is restored successfully.
  - **Failure** – Configuration restoration failed.
  - **Inprogress** – Configuration restoration is in-progress.
  - **Not Initiated** – Configuration restoration is not initiated.

- **Http Server Status** - Displays the status of the HTTP server as either enable or disable. The default option is **Enable**.

- **Http Port Number** - Displays the port to be used by the host to configure the router using the Web interface. This value ranges from 1 to 65535. The default value is **80**.

  Once the port number is changed, the Http Server Status is disabled and enabled. Open the HTTP session with IP address and new port number. For example, enter as 12.0.0.1:100, where 12.0.0.1 represents the IP of the switch and 100 represents the port number.

- **Telnet Status** - Select to set the status of TELNET in the system. The default option is **Disable**. The list contains the following;
  - **Enable** – Sets the Telnet status as enabled.
  - **Disable** – Sets the Telnet status as disabled.

- **Management Vlan ID** - Select the Management VLAN to be used for an IP connection to the switch from a workstation connected to a port in the VLAN. The default value of 1 allows an IP connection to be established through any port, but this may be changed if required to a different VLAN.

  Ensure that the VLAN to be configured as the management VLAN does exist, and the PVID of at least one port that is a port of the VLAN is the same as the management VLAN ID.

  Only one management VLAN can be active at a time.

  When a new management VLAN is configured, connectivity (to the GUI) through the existing management VLAN will be lost. The management workstation should be reconnected to the port in the new management VLAN.

Buttons	**Apply** - To modify attributes and save the changes

Chapter 9

User Management

To access User Management screen, click **System > User Management**.

9.1 User Management

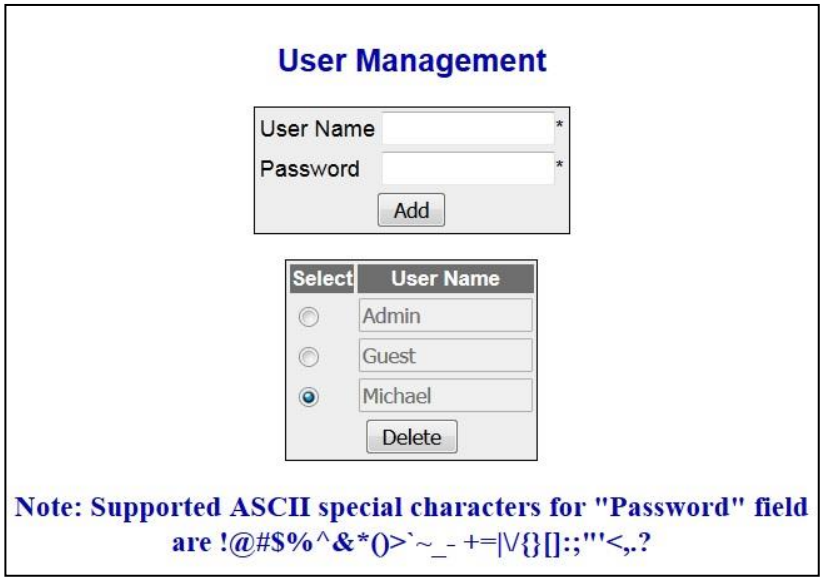


Figure 9-1 : User Management

Screen Objective

This screen allows the user to add and remove authorised users who can then access the switch.

- In this software release it is not possible to give each user different access privileges - every user will have full read/write access to all features of the switch..
- The default user name & password is **Admin**, **Admin**. However once the default "Admin" password has been succesfully changed, it is not possible to revert it back to "Admin" because there is a new restriction on password characters used that "Admin" does not meet. Yes - weird but true. We will change this in a future release.
- This default password change can be reversed by using the rear button reset - but this will also revert all switch parameters back to their default values.

Navigation

System > User Management

Fields

- **User Name** - Enter the required user name to add or change. This may be either an pre-existing user or a new user.
- **Password** - Enter the password required for the new or Existing user.
  - The Password must comprise of at least 5 ASCII characters.

The Password must include at least one numeric, one upper-case character, one lower-case character and one special **ASCII** character as defined as follows **:** !@#$%^&*()>`~_- +=|\/{}[]:;'"<,.?

Buttons	**Add** - Add the new user & password to the list or change the existing user's password. **Delete** - Add the new user & password to the list or change the existing user's password.

Chapter 10

Save and Restore

The **Save and Restore** link allows the user to configure the current configuration Save and Restore options for the switch:

To access Save and Restore screens, click **System > Save and Restore**.

The **Save and Restore** parameters are configured through the screens displayed by the following tabs:

- Save
- Restore
- File Download

By default the tab **Save** displays the **Save Configuration** screen.

10.1 Save Configuration

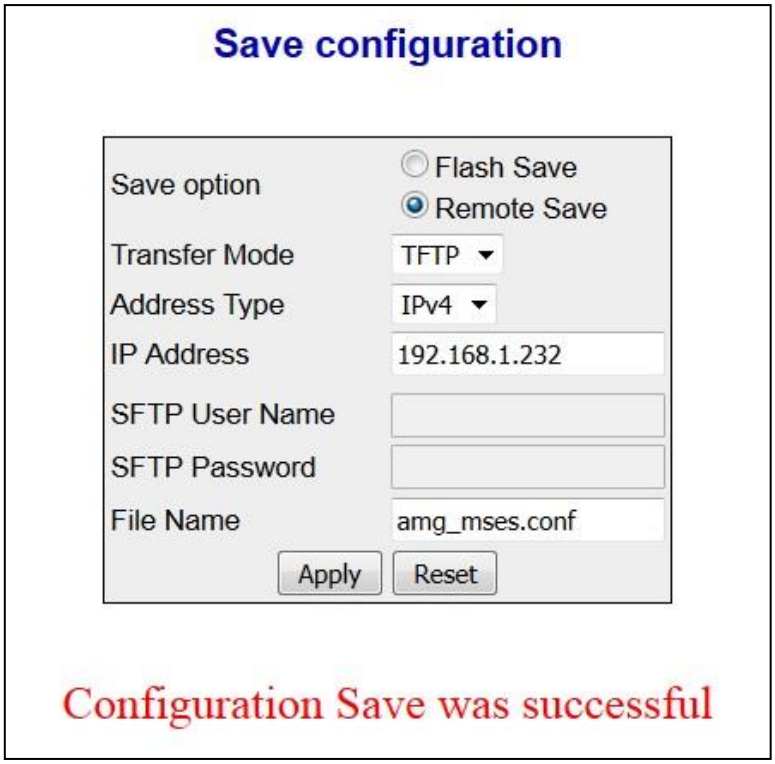


Figure 10-1 : Save configuration

Screen Objective	This screen allows the user to save the current configuration of the AMG 9IM2x/9HM2x Switch in a file. When save operation is initiated, all configurations made through CLI, SNMP or WEB interfaces are saved in a file (default name is **amg_mses.conf**). There are two options to save the configuration data namely, **Flash Save** and **Remote Save**. A Flash Save Configures that the configurations need to be saved in Flash whereas a Remote Save specifies that the configurations need to be saved to a remote system.
Navigation	**System > Save and Restore > Save**
Fields	• **Save option** - Click one of the option buttons to specify the save option to be used for the Switch. The options are: – Flash Save – Saves the configurations in the specified file name of Flash – Remote Save – Saves the configurations in the remote system which is specified by **Address Type** and **IP address** • **Transfer Mode** - Select the transfer mechanism to save the Switch configurations in the remote system. The remote host machine should have

a TFTP / SFTP capable Server running for this operation to be successful. The default option is **TFTP**. The list contains:

- TFTP – Saves the Switch configurations to the remote system through TFTP (Trivial File Transfer Protocol) mode.
- SFTP – Saves the Switch configurations to the remote system through SFTP (SSH File Transfer Protocol) mode.

This field is configurable only if the Save Option is set as Remote Save.

- **Address Type** - Select the IP Address type of the remote system in which the Switch configurations are to be saved. The default option is **IPv4**. The list contains:
  - IPv4 – Sets the Address type as IPv4.
  - IPv6 – Sets the Address type as IPv6.

  This field is configurable only if the Save Option is set as Remote Save.

- **IP Address** - Enter the IP Address of the remote system in which the Switch configurations are to be saved.

  This field is configurable only if the Save Option is set as Remote Save.

- **SFTP User Name** - Enter the user name required for saving the Switch configurations to the remote system in SFTP mode. This field is a string of maximum size 20

  This field is configurable only if the Save Option is set as Remote Save and the Transfer Mode is set as SFTP.

- **SFTP Password** - Enter the password required for saving the Switch configurations on to the remote system in SFTP mode. This field is a string of maximum size 20. The specified SFTP username / password should have been configured in the SFTP server running the remote station, for the remote save operation through SFTP to be successful.

  This field is configurable only if the Save Option is set as Remote Save and the Transfer Mode is set as SFTP.

- **File Name** - Displays the name of the file in which the Switch configurations are to be saved. The default file name where the Switch configurations are saved is **amg_mses.conf**. All configurations are saved in a single configuration file only.

  This file name is used for saving the Switch configuration, irrespective of the configuration **Save Option** which can be Flash or Remote Save.

Buttons

- **Apply** - To modify attributes and save the changes.
- **Reset** - To reset to default value for respective fields and discard all user inputs.

10.2 Restore Configuration

Figure 10-2 : Restore configuration

Screen Objective	This screen allows the user to restore the previously saved configurations of the Switch from the **Startup Configuration File**
Navigation	**System > Save and Restore > Restore**
Fields	• **Restore option** - Click one of the option buttons to specify whether the Switch configurations have to be restored. The list contains: – **No Restore** – Specifies that the switch configurations need not be restored when the system is restarted – **Flash Restore** – Restores the configurations from the **Startup Configuration File** in the Flash, when the system is restarted.
Buttons	• **Apply** - To modify attributes and save the changes. • **Reset** - To reset to default value for respective fields and discard all user inputs.

10.3 File Download

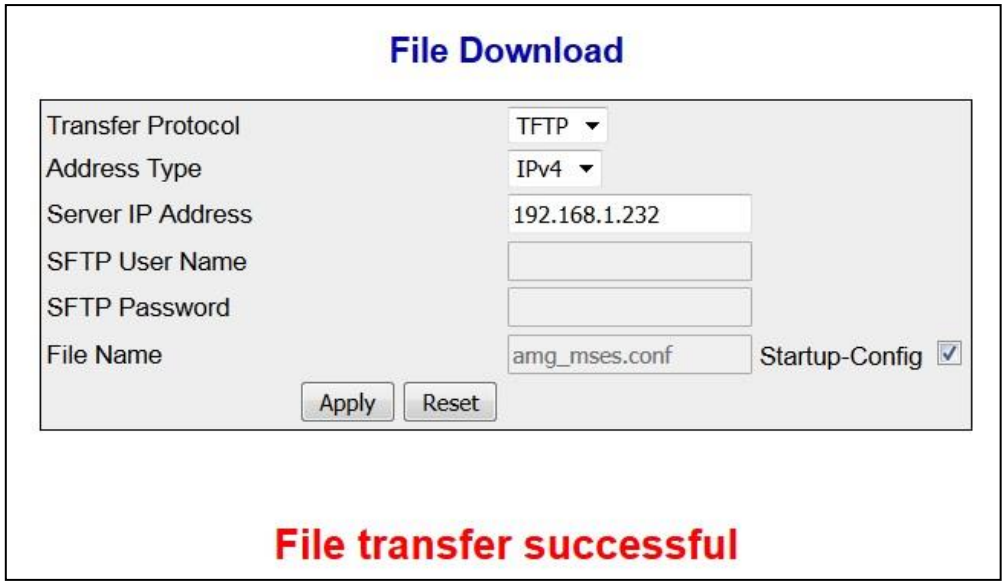


Figure 10-3 : File Download

Screen Objective	This screen allows the user to configure the file download details
Navigation	**System > Save and restore > File Download**
Fields	• **Transfer Protocol** - Select the transfer mode for downloading file from the remote system. The default option is **TFTP**. The list contains: – TFTP – Specifies that transfer mode for downloading file from the remote system is TFTP (Trivial File Transfer Protocol) – SFTP – Specifies that transfer mode for downloading file from the remote system is SFTP (SSH File Transfer Protocol)... • **Address Type** - Enter the Ip Address of machine to which the log file is to be downloaded. The Options are – IPV4 - Sets the IP Address type as IPV4. – IPV6 - Sets the IP Address type as IPV6 • **Server IP Address** - Enter the IP address of the machine from which the file is to be downloaded. • **SFTP User Name** - Enter the user name required for downloading the file in SFTP mode. This field is a string with the maximum size 20. This field is disabled if the Transfer Protocol is selected as TFTP. • **SFTP Password** - Enter the password required for downloading the file in SFTP mode. This field is a string with the maximum size 20. This field is disabled if the Transfer Protocol is selected as TFTP.

	• **File Name** - Enter the name of the file to be downloaded from the remote system. • **Startup config** - Select the function Startup configuration. A startup configuration contains configuration information that the AMG 9IM2x/9HM2x uses at reboot. This command retrieves a backup of the initial configuration from flash or a remote location to use it for restoration.
Buttons	• **Apply** - To modify attributes and save the changes. • **Reset** - To reset to default value for respective fields and discard all user inputs.

Chapter 11

Software Upgrade

To access Software Upgrade screen, click **System > Software Upgrade**

11.1 Software Upgrade

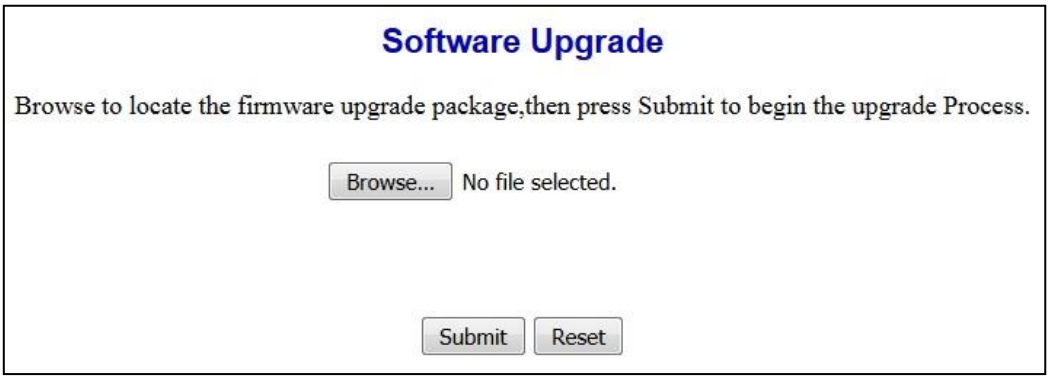


Figure 11-1 : Software Upgrade

Screen Objective	This screen allows the user to perform a combined firmware download & upgrade operation on a switch stack or standalone switch by downloading a new upgrade pack (image file) from a local PC drive, USB key, or Ethernet directory / location to the switch and overwriting and updating the existing firmware. The only web browser approved for the software upgrade procedure at the current time is Microsoft Internet Explorer 11. The software upgrade pack will be in compressed file format (.tar.gz) and typically named "M.SES Release 2.x.x.tar.gz"
Navigation	**System > Software Upgrade**
Fields	• **Browse** - Select the path / name of the upgrade pack to be downloaded. • **Blank** - The path / name of the selected upgrade pack.
Buttons	**Submit** - Confirm the selected upgrade pack and start the download & upgrade process. The user should wait for 1-2 minutes once the file download has started. A warning message will flash alternately red & brown to indicate this process is progressing. Do NOT re-boot or re-power the switch at this time. After the upgrade pack has been succesfully download, there may be a small period of time 5-10 seconds whilst the image file is unpacked and installed before a confirmation message appears. Do NOT re-boot or re-power the switch at this time. WAIT for the confirmation message to appear. **Reset** - Clear the current selected upgrade pack.

Screen Objective	The following information screen informs the user that the upgrade pack (image) download is in progress.

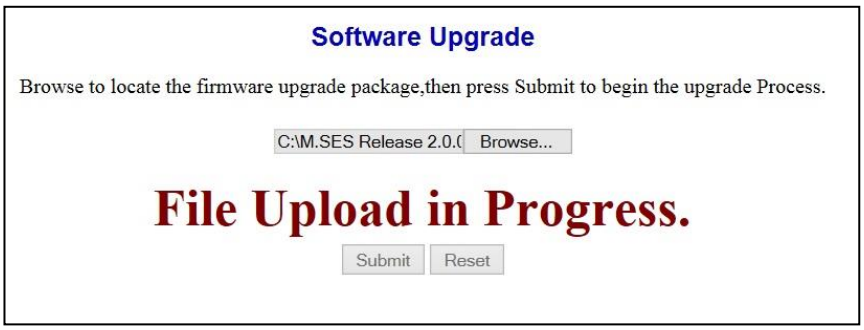


Figure 11-2 : Software Upgrade : File Upload in Progress

Screen Objective	The following screen informs the user that the upgrade pack (image) has sucesfully been downloaded and the upgrade has been completed.

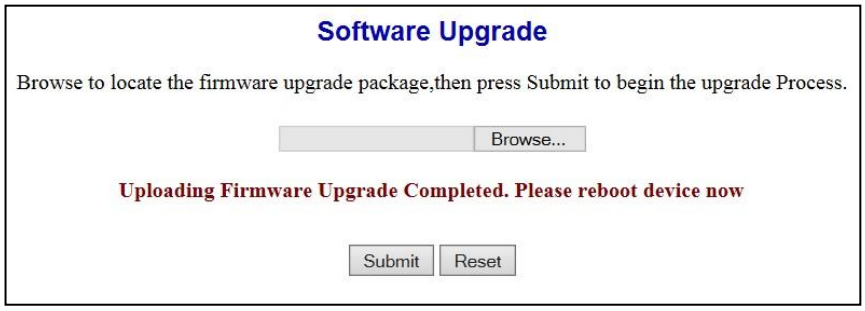


Figure 11-3 : Software Upgrade : File Upload Completed

The user should now re-boot or re-power the switch at this time.

Chapter 12

Reboot

To access Reboot screen, click **System > Reboot**

12.1 Reboot

Figure 12-1 : Rebooting the System

Screen Objective	This screen allows the user to restart the switch/ target... The user should wait for 2 minutes before logging in after reboot. All updates to nvram.file using the screen **System > NVRAM Settings > Factory Default Settings** are effective only after reboot
Navigation	**System > Reboot**
Buttons	**Reboot** - To restart the switch.

Chapter 13

SNTP

SNTP (Simple Network Time Protocol) is a simplified version of the NTP protocol. The NTP protocol is meant for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.

To access SNTP screens, click **System > SNTP**.

The **File Transfer** parameters are configured through the screens displayed by the following tabs:

- SNTP Global
- SNTP Unicast Mode

By default the tab **SNTP** displays the **SNTP Global Configuration** screen.

13.1 SNTP Global Configuration

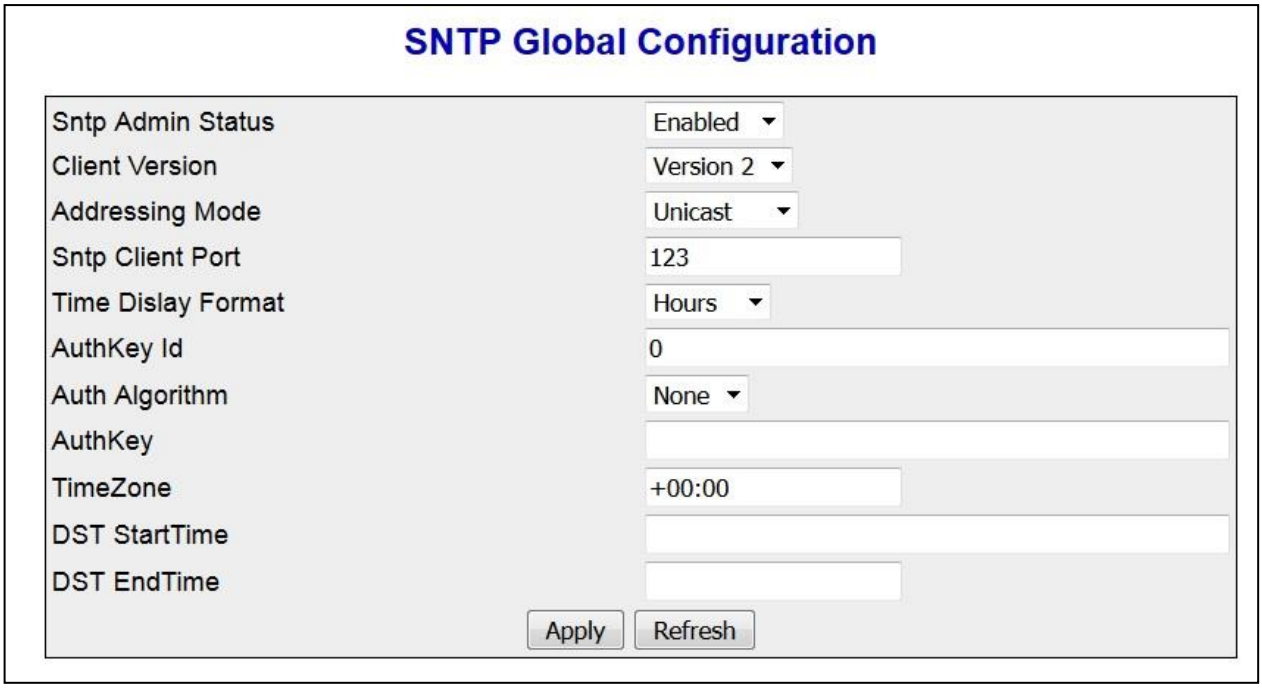


Figure 13-1 : SNTP Global Configuration

Screen Objective	This screen allows the user to configure the details of SNTP scalars
☞	To set the system time using SNTP, the Clock Time source should be configured as NTP.
Navigation	**System > SNTP > SNTP Global**
Fields	• **Sntp Admin Status** - Select the SNTP client module status. The default option is **Disabled**. The list contains: – Enabled – Enables the SNTP client module. On enabling, the server starts sending the request to the host for synchronization. – Disabled – Disables the SNTP client module. ✎ All the configurations are active only when the SNTP module is enabled. • **Client Version** - Select the SNTP client module version. The default option is **Version 4.** The list contains: – Version 1 - Sets the SNTP client version as Version 1 – Version 2 - Sets the SNTP client version as Version 2 – Version 3 – Sets the SNTP client version as Version 3 – Version 4 – Sets the SNTP client version as Version 4

All the SNTP requests are sent out with the current configured version number. When required, the administrator can change the current version number.

- **Addressing Mode** - Displays the SNTP client addressing mode. The only option is **Unicast**.

  Unicast - SNTP client operates in a point-to-point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally, the round-trip delay and local clock offset relative to the server.

- **Sntp Client Port** - Enter the SNTP client port number. This value ranges from 1025 to 65535. The default value is 123.

- **Time Dislay Format** - Select the time display format. The default option is **Hours.** The list contains:
  - Hours – Sets the time display as 24 hours format.
  - Am/Pm – Sets the time display as 12 hours AM/PM format.

- **AuthKey Id** - Enter the key identifier identifying the cryptographic key used to generate the message-authentication code.

- **Auth Algorithm** - Select the SNTP authentication algorithm. The default authentication algorithm is **None.** The list contains:
  - None – The communication will be opened and no authorization will be provided.
  - md5 - MD5 (Message Digest-5) verifies data integrity. MD5 is intended for use with digital signature applications, which requires that large files must be compressed by a secure method before being encrypted with a secret key, under a public key cryptosystem.

- **AuthKey** - Enter the authentication key that is used to implement NTP authentication.

- **TimeZone** - Enter the system time zone with respect to UTC. The format is (+/-)HH:MM. Where:
  - +/- denotes the difference with the Greenwich Mean Time. + indicates forward time zone and - indicates backward time zone.
  - HH denotes the hours. It is 24-hour format with value ranging from 00 to 23.
  - mm denotes the minutes. The value ranges from 00 to 59. For example, the valid value is +05:30.

- **DST StartTime** - Enter the DST (Daylight Saving Time) start time. The format is weekofmonth-weekofday-month,HH:MM. Where:
  - Weekofmonth denotes the particular week. The valid values are First, Second, Third, Fourth and Last.
  - weekofday denotes the day in the specified week. The valid values are Sun, Mon, Tue, Wed, Thu, Fri and Sat.

- month denotes the month for which the specified week and day are applicable. The valid values are Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec
- HH denotes the hours. It is 24-hour format with value ranging from 00 to 23.
- mm denotes the minutes. The value ranges from 00 to 59. For example, the valid value is First-Sun-Jan, 23:45.

> DST is a system of setting clocks ahead so that both sunrise and sunset occur at a later hour. The effect is additional daylight in the evening. Many countries observe DST, although most have their own rules and regulations for when it begins and ends. The dates of DST may change from year to year.

- **DST EndTime** - Enter the DST end time. The valid format is [weekofmonth-weekofday-month, HH:MM]. The format is weekofmonth-weekofday-month,HH:MM. Where:
  - weekofmonth denotes the particular week. The valid values are First, Second, Third, Fourth and Last.
  - weekofday denotes the day in the specified week. The valid values are Sun, Mon, Tue, Wed, Thu, Fri and Sat.
  - month denotes the month for which the specified week and day are applicable. The valid values are Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec
  - HH denotes the hours. It is 24-hour format with value ranging from 00 to 23.
  - mm denotes the minutes. The value ranges from 00 to 59. For example, the valid value is First-Mon-Jan,23:45.
  -

Buttons

- **Apply** - To add and save new configuration.
- **Reset** - To reset to default value for respective fields and discard all user inputs.

13.2 SNTP Unicast Mode Configuration

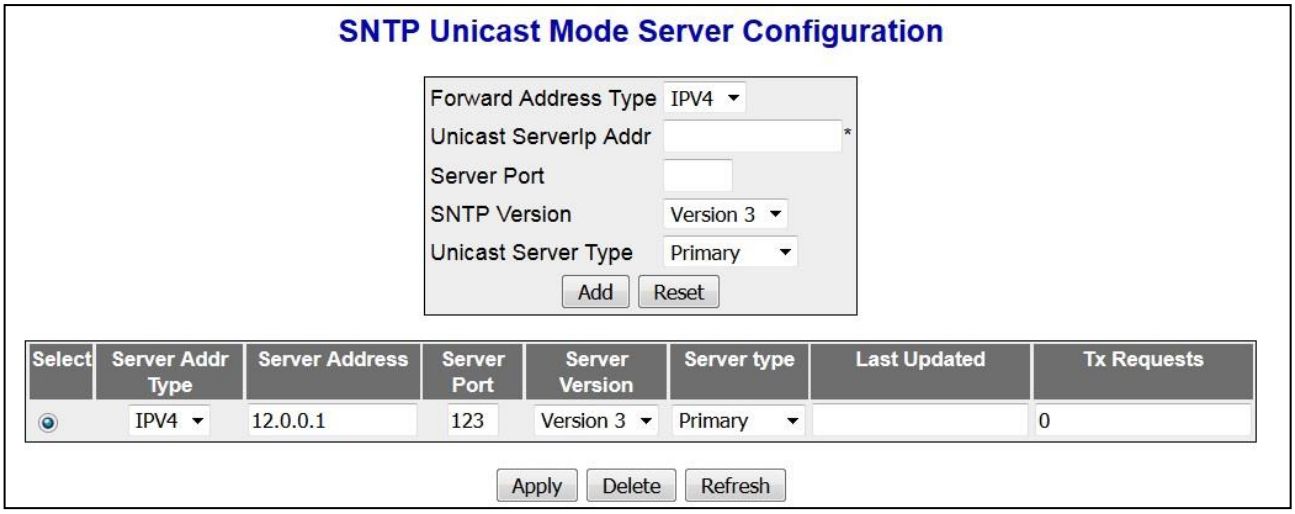


Figure 13-2 : SNTP Unicast Mode Configuration

Screen Objective	This screen allows the user to configure the SNTP unicast parameter.
Navigation	**System** > **SNTP > SNTP Unicast Mode**
Fields	• **Select** - Click to select the server address for which the configuration need to be modified or deleted. • **Forward Address Type** - Select the address type of the unicast server in the Unicast addressing mode. The list contains: – IPV4 – Sets the address type of the unicast server as Internet Protocol Version 4 – IPV6 - Sets the address type of the unicast server as Internet Protocol Version 6 • **Unicast ServerIp Addr** - Enter the unicast IPv4/IPv6 server address in the Unicast addressing mode. • **Server Port** - Enter the SNTP port on which the server is UP. The value ranges between 123, 1025 to 65535. The default value is **123**. • **SNTP Version** - Select the SNTP version supported by the server. The list contains: – Version 3 – Sets the SNTP version as version 3. – Version 4 – Sets the SNTP version as version 4. • **Unicast Server Type** - Select the Unicast server type. This flag is to distinguish between primary and secondary server. SNTP client sends request to different servers until it receives successful response. This flag tells the order in which to query the servers The list contains:

	– Primary – Sets the unicast server type as primary server – Secondary – Sets the unicast server type as secondary server • **Last Updated** - Specifies the local time when the system time was successful. • **Tx Requests** - Specifies the number of SNTP requests sent in the Unicast addressing mode.
Buttons	• **Add** - To add and save new configuration. • **Reset** - To reset to default value for respective fields and discard all user inputs. • **Apply** - To modify attributes for the selected entry and save the changes. • **Delete** - To delete the selected entry. • **Refresh** – To refresh the screen

Chapter 14

HTTP

HTTP (Hyper Text Transfer Protocol) 1.1 Server provides an HTTP Authentication framework in addition to the proprietary form-based authentication. The HTTP authentication framework provides a simple challenge-response authentication mechanism that is used by a server to challenge a client request and by a client to provide authentication information. The HTTP related parameters are configured through the screen displayed by the following tab:

- Session Timeout

14.1 HTTP Session Timeout

Figure 14-1 : HTTP Session Timeout

Screen Objective	This screen allows the user to configure the web session time out value.
Navigation	**System > HTTP > Session Timeout**
Fields	• **Web Session Timeout** - Enter the web session timeout value in seconds.. This value ranges from 1 to 3600 in seconds. The default value is **360** (6 minutes).
Buttons	**Apply** - To modify attributes and save the changes.

PoE

PoE (Power Over Ethernet). The PoE related parameters are configured through the screen displayed by the following tab:

- PoE Manager

15.1 PoE Manager

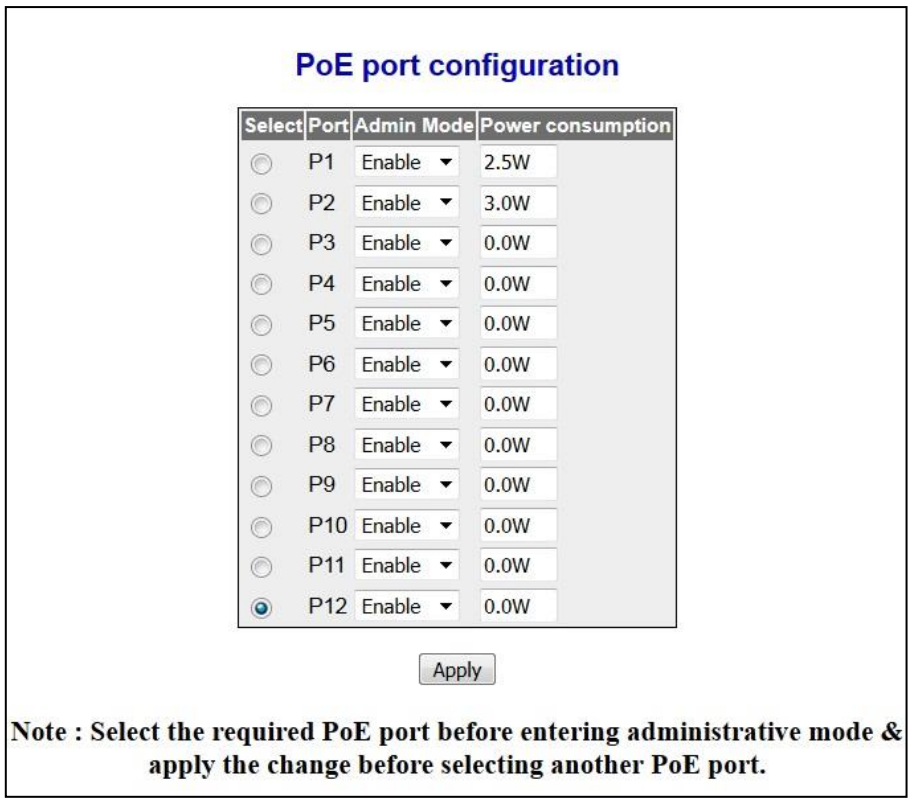


Figure 15-1 : PoE Port Configuration

Screen Objective	This screen allows the user to enable or disable the PoE outputs on a per port basis. It also shows the current PoE power (in W) currently being provided to the load on each RJ45 Ethernet port.
Navigation	**System > PoE > PoE interface**
Fields	• **Select** - Click to select the port to be configured. • **Port** - Displays the port from P1-P24. • **Admin Mode** - Select the PoE output mode. The default option is **Enable**. The list contains : **Enable** – Port provides PoE power. **Disable** – Port does not provide PoE power. • **Power Consumption** - PoE power being suppled (W) per port
Buttons	**Apply** - To modify attributes and save the changes.

Chapter 15

SNMP

SNMP (Simple Network Management Protocol) is a widely deployed protocol that is commonly used to monitor and manage network devices. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called Agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

To access SNMP screens, click **System > SNMP**

SNMP link also allows the user to configure SNMP Agent parameters through the following sub-links.

- SNMP Agent Control Settings
- SNMP Global Configuration
- SNMP Agent
- SNMP Proxy

By default, the **SNMP** link displays the **SNMP Agent Control Settings** screen.

16.1 SNMP Agent Control Settings

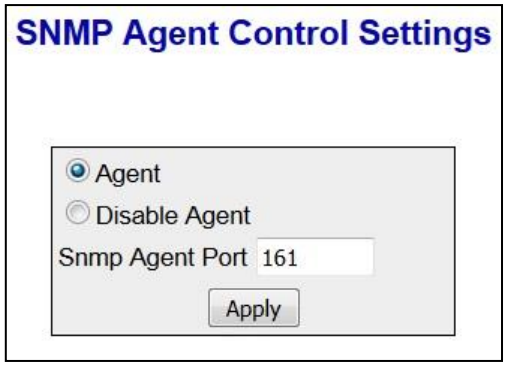


Figure 16-1 : SNMP Agent Control Settings

Screen Objective	This screen allows the SNMP user to configure SNMP Agent Control Settings.
Navigation	**System > SNMP> Agent Control**
Fields	• **Agent** - Select Agent to enable the SNMP Agent. This allows the software to directly interface with the managed modules to configure and monitor them. The default option is enabled. • **Disable Agent** - Select Disable to disable SNMP Agent. • **Snmp Agent Port** - Enter the SNMP Agent Port number on which snmp Agent listens. This value ranges from 1 to 65535. The default value is 161. This field is greyed out for **Disable Agent** option.
Buttons	**Apply** - To modify attributes and save the changes.

16.2 SNMP Global Configuration

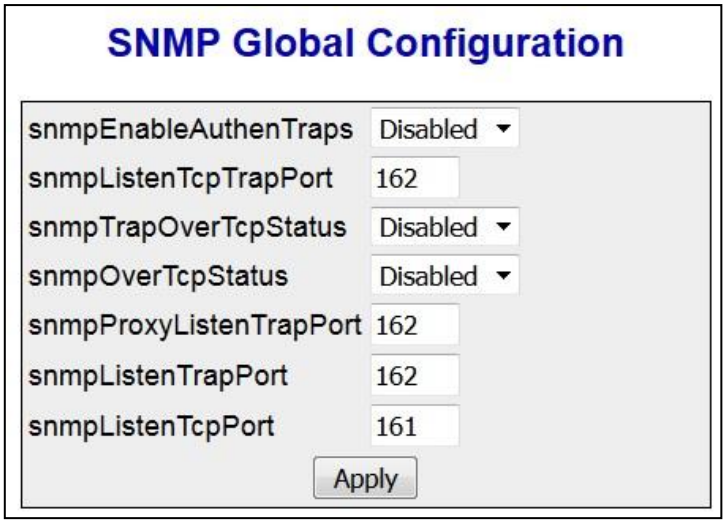


Figure 16-2 : SNMP Basic Settings

Screen Objective	This screen allows the user to configure SNMP scalar parameters which are independent of each other
Navigation	**System > SNMP > SNMP Global Configuration**
Fields	• **snmpEnableAuthenTraps** - Select the status of the authentication failure traps. The list contains: – Enabled – Enables the generation of authentication failure traps. – Disabled – Disables the generation of authentication failure traps. • **snmpListenTcpTrapPort** - Enter the port number on which SNMP trap message are sent to the manager over TCP. The default value is **162**. • **snmpTrapOverTcpStatus** - Select the status of sending SNMP trap messages over TCP. The list contains: – Enables – Allows sending of SNMP trap messages over TCP. – Disables – Blocks sending of SNMP trap messages over TCP. • **snmpOverTcpStatus** - Select the status of sending SNMP messages over TCP. The list contains: – Enables – Allows sending of SNMP messages over TCP. All SNMP messages are sent over TCP instead of UDP. – Disables - Blocks sending of SNMP messages over TCP. • **snmpProxyListenTrapPort** - Enter the port number on which proxy listens for trap and inform messages from the Agent. The default value is **162**.

	• **snmpListenTrapPort** - Enter the port number on which SNMP trap messages are sent to the manager. The default value is **162**. • **snmpListenTcpPort** - Enter the port number on which SNMP trap messages are sent to the manager over TCP. The default value is **161**.
Buttons	**Apply** - To modify attributes and save the changes.

16.3 SNMP Agent Configuration

SNMP Agent Configuration provides an interface between a SNMP manager and a switch. The Agent processes SNMP packets received from the manager, frames the appropriate response packets and sends them to the manager.

To access SNMP Agent Screens, click **System** > **SNMP > Agent Config.**

The **SNMP Agent Config.** link allows the user to configure SNMP Agent related parameters through the following tabs:

- Community Settings
- Group Settings
- Group Access
- View
- Target Address
- Target Parameter
- User
- Trap Manager
- Filter Conf

By default, the tab **Agent Config.** displays **SNMP Community Settings** screen.

16.3.1.1 SNMP Community Settings

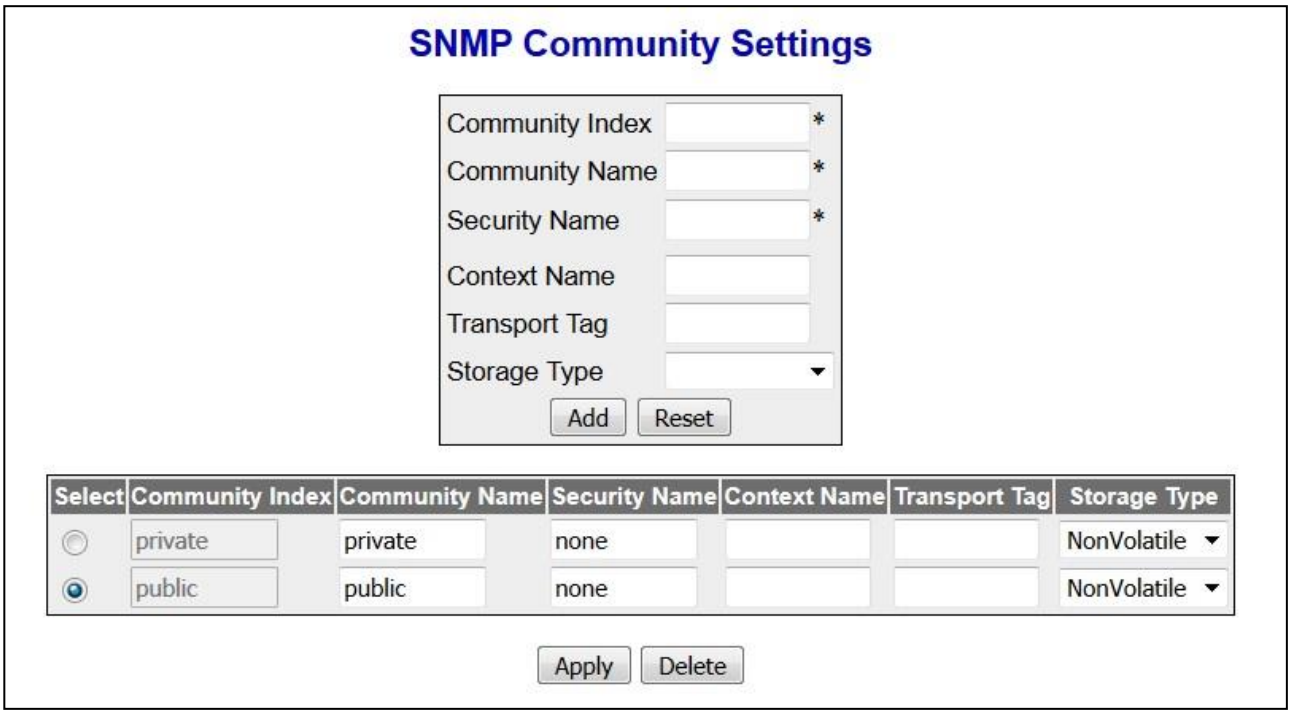


Figure 16-3 : SNMP Community Settings

Screen Objective	This screen allows the user to add new community configuration to the table and delete existing community configuration from the same
Navigation	**System** > **SNMP > Agent Config. > Community**
Fields	• **Community Index** - Enter the Index to the community table. The communities private and public are created, once the M-SES is started to provide SNMP access to the M-SES. • **Community Name** - Enter the community name. The communities private and public are created, once the M-SES is started to provide SNMP access to the M-SES. • **Security Name** - Enter the security name. The default value is None. • **Context Name** - Enter the context name. The default value is Null. • **Transport Tag** - Enter the transport tag. The default value is Null. • **Storage Type** - Select the required Storage type for the community. The default options is **Non**Volatile. The list contains: – Volatile – Sets the storage type as temporary and erases the configuration setting on restarting the system.

	– Non Volatile – Sets the storage type as permanent and saves the configuration to the system. You can view the Saved configuration on restarting the system.
Buttons	• **Add** - To add and save new configuration. • **Reset** - To reset to default value for respective fields and discard all user inputs. • **Apply** - To modify attributes for the selected entry and save the changes. • **Delete** - To delete the selected entry.

16.3.1.2 SNMP Group Settings

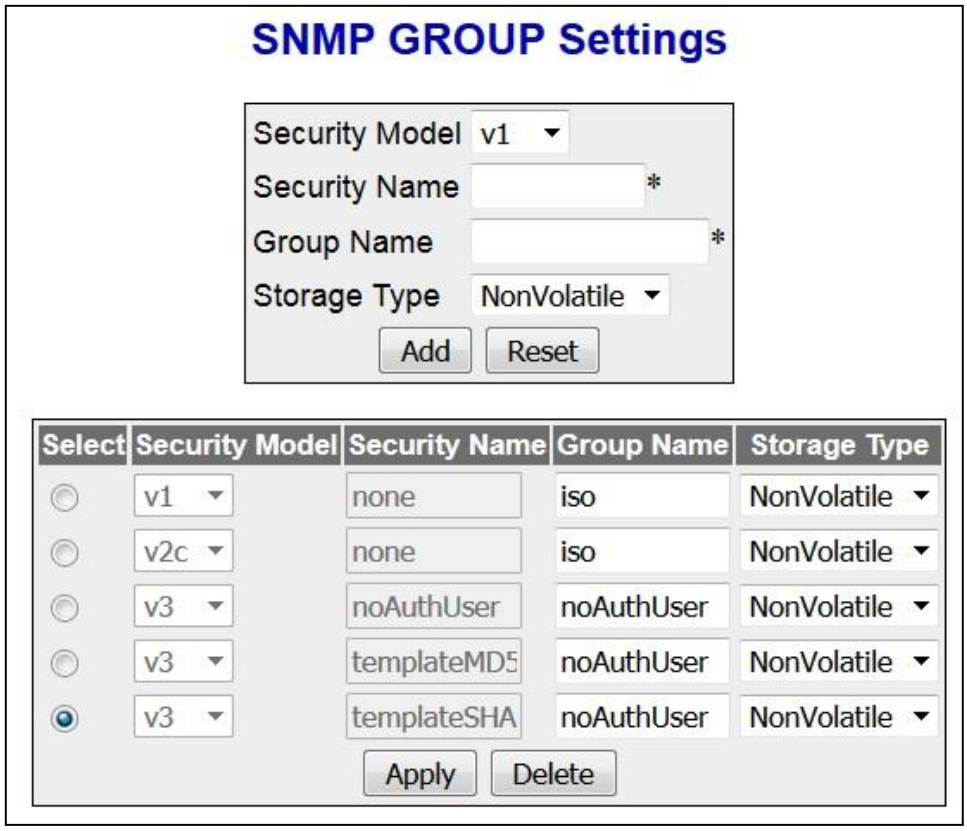


Figure 16-4 : SNMP GROUP Settings

Screen Objective	This screen allows the user to configure the SNMP Group Settings
Navigation	**System** > **SNMP > Agent Config. > Group**
Fields	• **Security Model** - Select the version of the SNMP. The security model v1, v2c and v3 are created, once the M-SES is started. The list contains: – v1 – Sets the SNMP version as Version 1. – v2c – Sets the SNMP version as Version 2. – v3 – Sets the SNMP version as Version 3. Group Name and Storage Type are created when M-SES is started Group Name and Storage Type can be modified for the default entries. Default entries cannot be deleted. • **Security Name** - Enter the security name of the group. The security name none, noAuthUser, templateMD5 and templateSHA are created, once the M-SES is started.This is a Read only field.

	• **Group Name** - Enter the name of the SNMP group. The SNMP groups iso and initial are created, once the M-SES is started. • **Storage Type** - Select the required Storage type for the group entry. The default option is **NonVolatile** The list contains: – Volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system. – Non Volatile – Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.
Buttons	• **Add** - To add and save new configuration. • **Reset** - To reset to default value for respective fields and discard all user inputs. • **Apply** - To modify attributes for the selected entry and save the changes. • **Delete** - To delete the selected entry.

16.3.1.3 SNMP Group Access Settings

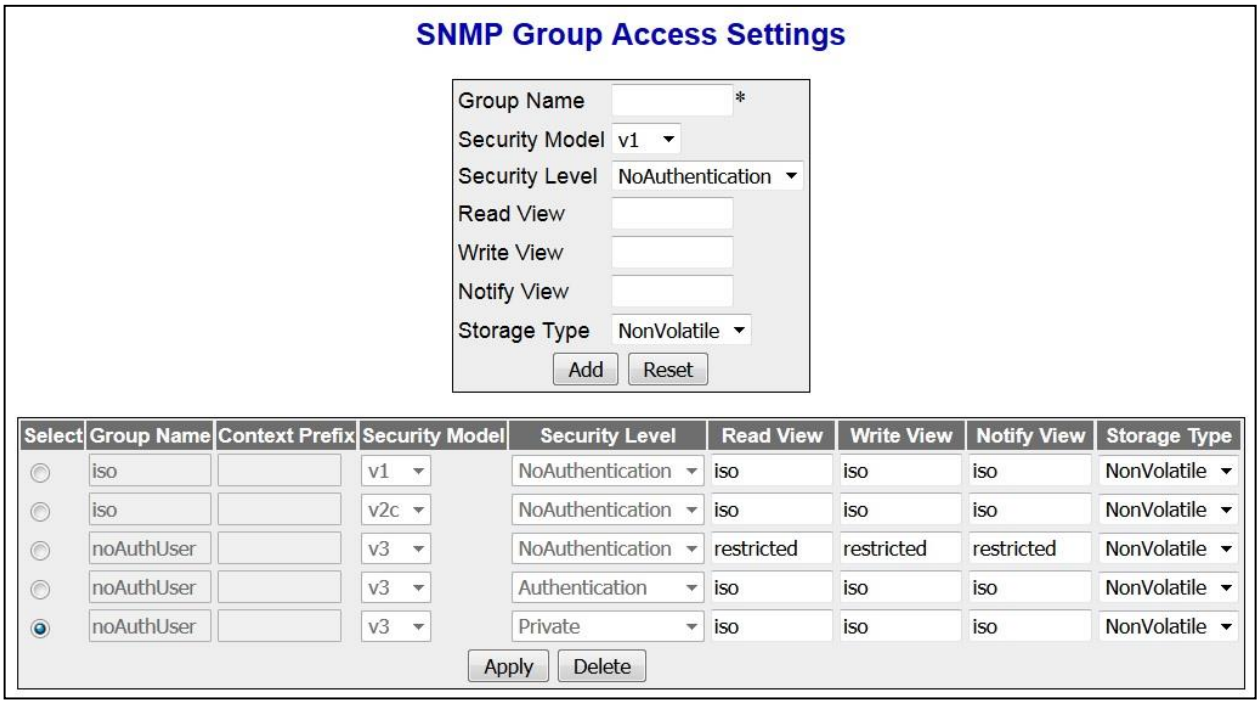


Figure 16-5 : SNMP Group Access Settings

Screen Objective	This screen allows the user to configure SNMP Group Access Settings
☞	A **SNMP Group** has to be created prior to the Group Access configuration. The groups that are created in the SNMP Group Settings section are displayed in the bottom form of this screen.
Navigation	**System** > **SNMP > Agent Config. > Group Access**
Fields	• **Group Name** - Enter the name of the group. The maximum size is 32. • **Security Model** - Select the version of the SNMP. The list options are: – v1 – Sets the SNMP version as Version 1. – v2c – Sets the SNMP version as Version 2. – v3 – Sets the SNMP version as Version 3. • **Security Level** - Select the version of the SNMP. The list contains: – NoAuthentication – Sets no authentication – Authentication - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication. – Private – Sets both authentication and privacy.

	• **Read View** - Enter the read view identifier from which the user can read the data. The maximum size is 32. • **Write View** - Enter the write view identifier from which the user has both the read and write access. The maximum size is 32. • **Notify View** - Enter the notify view identifier. From this identifier number the changes made will be noted and sent to a destination through a tag. The maximum size is 32. • **Storage Type** - Select the required Storage type for the group access entry. The list contains: – Volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system. – Non Volatile – Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.
Buttons	• **Add** - To add and save new configuration. • **Reset** - To reset to default value for respective fields and discard all user inputs. • **Apply** - To modify attributes for the selected entry and save the changes. • **Delete** - To delete the selected entry.

16.3.1.4 SNMP View Tree Settings

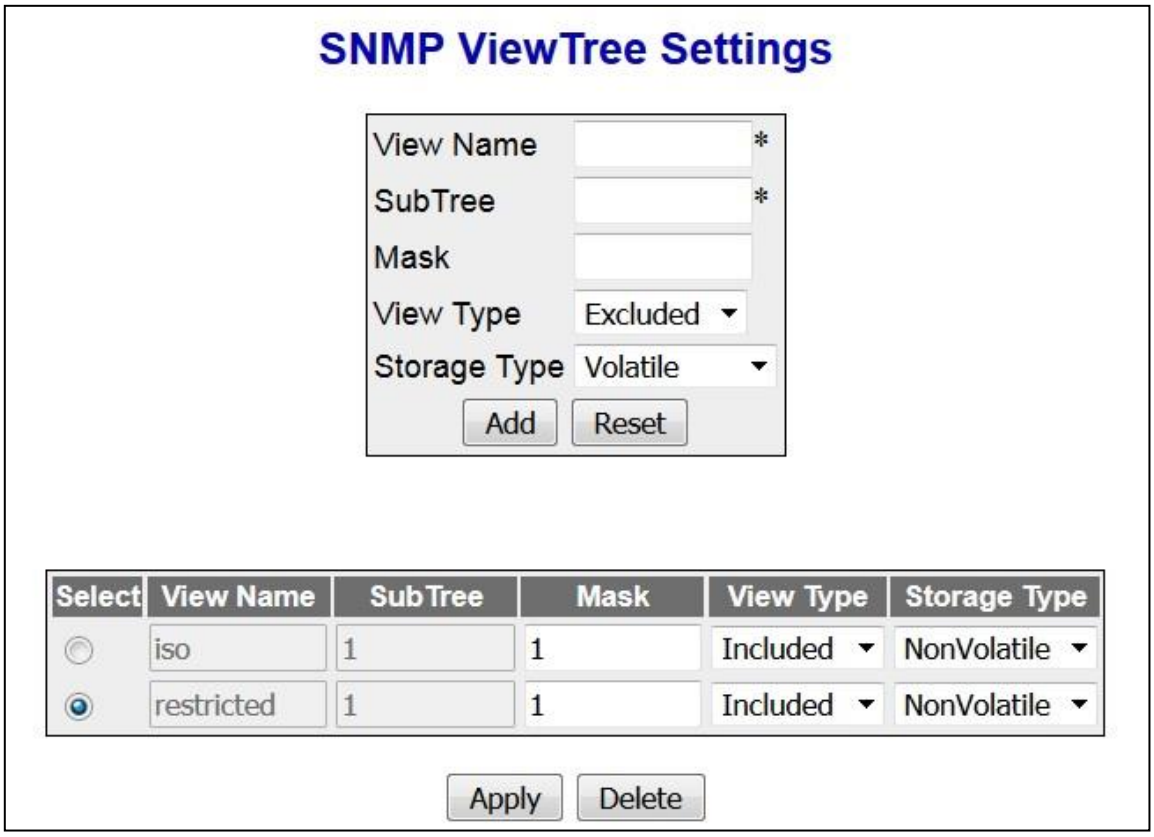


Figure 16-6 : SNMP View Tree Settings

Screen Objective	This screen allows the user to configure the SNMP ViewTree Settings
☞	**SNMP Group** has to be created and **SNMP Access** settings need to be defined prior to the Group View Tree configuration
Navigation	**System** > **SNMP > Agent Config. > View**
Fields	• **View Name** - Enter the View Name for which the view details are to be configured. The default option is ISO and restricted. The View name iso and restricted are created, once the M-SES is started. • **SubTree** - Enter the Sub Tree value for the particular view. The default value is **1**. • **Mask** - Enter the Mask value for the particular view. The default value is **1**. • **View Type** - Select the View Type. The default option is **Included** The list contains: – Included – Allows access to the subtree. – Excluded – Denies access to the subtree.

	• **Storage Type** - Select the required Storage type for the view tree entry. The default option is **NonVolatile** The list contains: – Volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system. – Non Volatile – Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.
Buttons	• **Add** - To add and save new configuration. • **Reset** - To reset to default value for respective fields and discard all user inputs. • **Apply** - To modify attributes for the selected entry and save the changes. • **Delete** - To delete the selected entry.

16.3.1.5 SNMP Target Address Settings

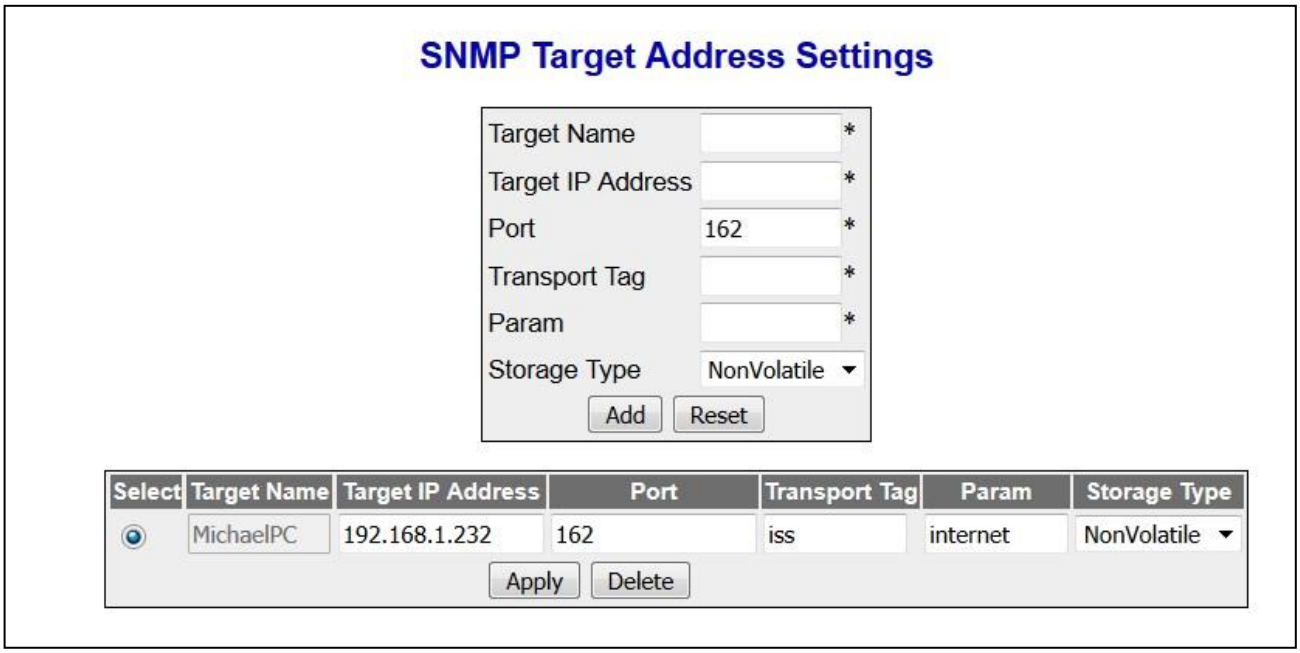


Figure 16-7 : SNMP Target Address Settings

Screen Objective	This screen allows the user to configure the SNMP Target Address Settings.
Navigation	**System** > **SNMP > Agent Config. > Target Address**
Fields	• **Target Name** - Enter a unique identifier for the Target. The maximum size is 32. • **Target IP Address** - Enter a target IP address to which the generated SNMP notifications are sent. • **Port** - Enter the port number through which the generated SNMP notifications are sent to the target address. • **Transport tag** - Enter the tag identifier that is used to select the target address for the SNMP notifications. This must be the same as the Notify Tag field in Trap Manager page. • **Param** - Enter SNMP parameters to be used when generating messages to be sent to transport address. This must be the same as the Parameter Name field in the SNMP Target Parameter page.The maximum size is 32. • **Storage Type** - Select the required Storage type for the target address entry. The list contains: – Volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system.

	– Non Volatile – Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.
Buttons	• **Add** - To add and save new configuration. • **Reset** - To reset to default value for respective fields and discard all user inputs. • **Apply** - To modify attributes for the selected entry and save the changes. • **Delete** - To delete the selected entry.

16.3.1.6 SNMP Target Parameter Settings

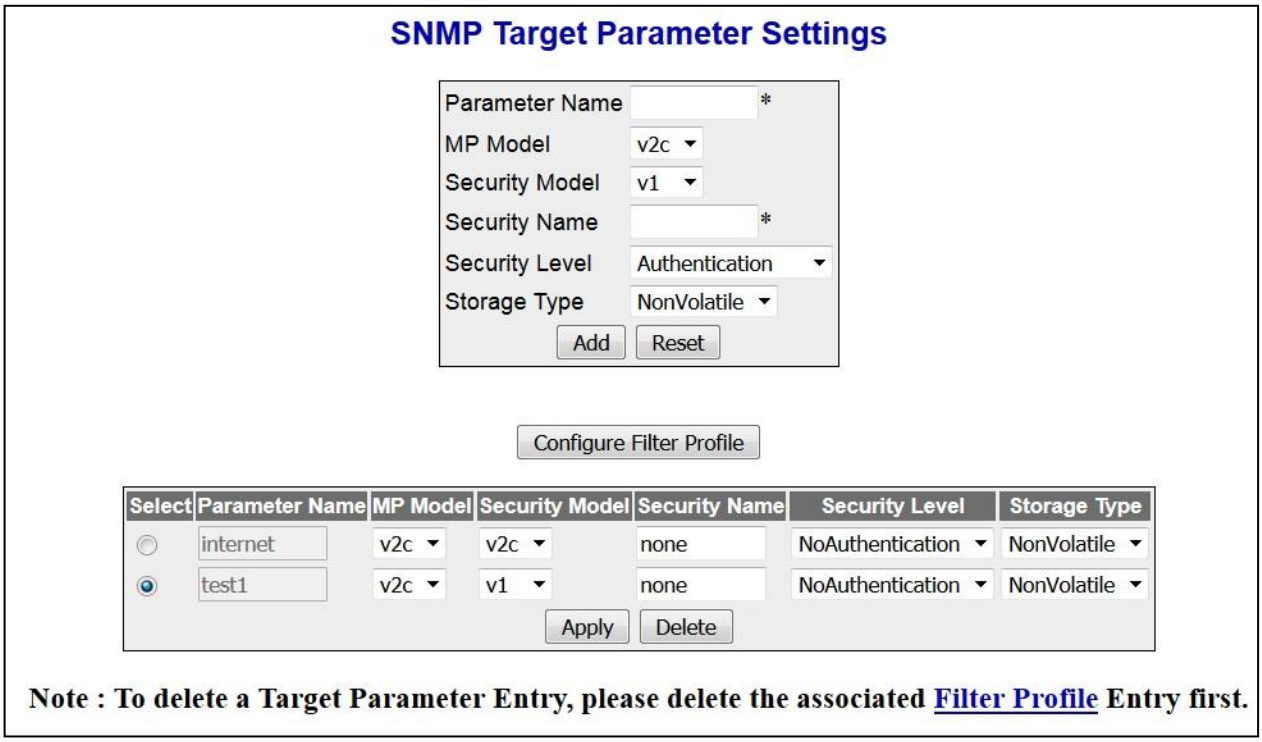


Figure 16-8 : SNMP Target Parameter Settings

Screen Objective	This screen allows the user to configure the SNMP target information to be used in the generation of SNMP messages
☞	The target parameter entry can be deleted only if the associated filter profile entry is deleted through the **Filter Profile Settings** screen
Navigation	**System** > **SNMP > Agent Config. > TargetParameter**
Fields	• **Parameter Name** - Enter a unique identifier of the parameter. The maximum size is 32. The default option is **Internet** • **MP Model** - Select the MP model of the SNMP. The default option is v2c. The list contains: – v1 – Sets the MP model as Version 1. – v2c – Sets MP model as Version 2. – v3 – Sets the MP model as Version 3. • **Security Model** - Select the version of the SNMP. The default option is v2c. The list contains: – v1 – Sets the security model as Version 1. – v2c – Sets the security model as Version 2.

- v3 – Sets the security model as Version 3.

- **Security Name** - Enter the security name to generate SNMP messages. The default option is **None** The maximum size is 32.

- **Security Level** - Select the level of security to be used when generating SNMP messages. The default option is **NoAuthentication** The list contains:
  - NoAuthentication – Sets no authentication.
  - Authentication - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication.
  - Private - Enables both authentication and privacy.

- **Storage Type** - Select the required Storage type for the target parameter entry. The default option is **NonVolatile**. The list contains:
  - Volatile – Indicates that the storage type is temporary. Erases the configuration setting on restarting the system.
  - Non Volatile – Indicates that the storage type is permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.

Buttons

- **Add** - To add and save new configuration.
- **Reset** - To reset to default value for respective fields and discard all user inputs.
- **Apply** - To modify attributes for the selected entry and save the changes.
- **Delete** - To delete the selected entry.
- **Configure Filter Profile** – To access **Filter Profile Settings** screen.

16.3.1.6.1 SNMP Filter Profile Settings

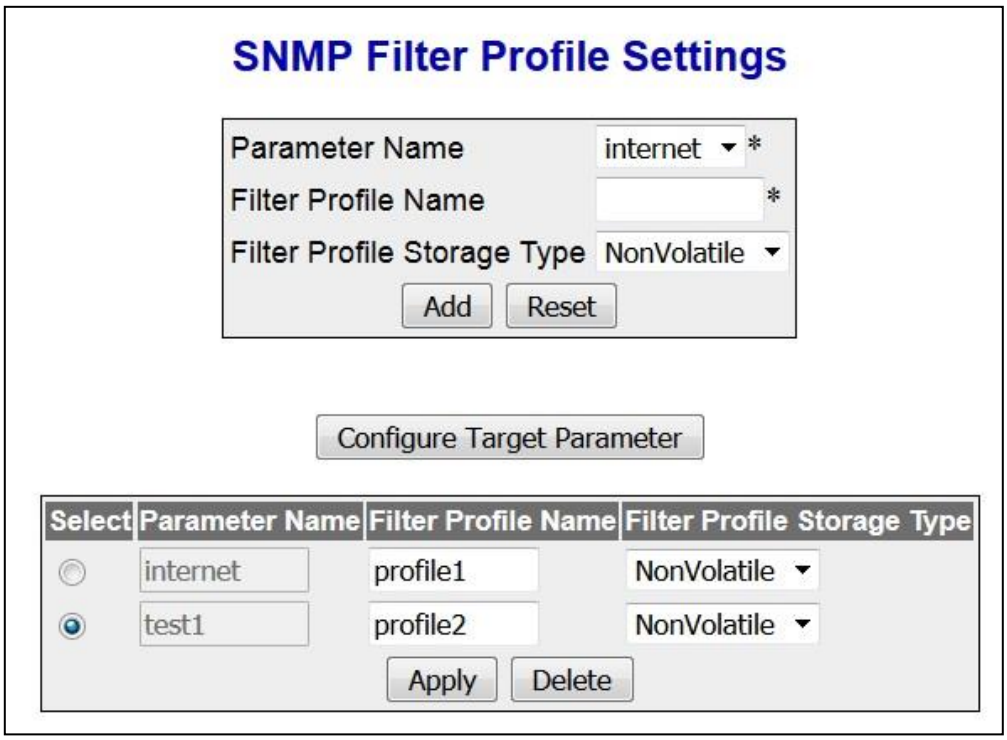


Figure 16-9 : SNMP Filter Profile Settings

Screen Objective	This screen allows the user to configure the filter profile to be used when generating notifications using the corresponding entry in the target parameters table
Navigation	**System** > **SNMP > Agent Config. > TargetParameter > SNMP Target Parameter Settings** screen **>** click **Configure Filter Profile** button,
Fields	• **Parameter Name** - Select the existing parameter name to which the filter profile setting should be assigned. • **Filter Profile Name** - Enter the name for the filter profile. This name is used when generating notifications using the corresponding entry in the target address table. This value is a string of maximum size of 32. • **Filter Profile Storage Type** - Select the storage type for the filter profile entry. The defsult option is **NonVolatile**. The list contains: – Volatile - Sets the storage type as temporary. Erases the configuration setting on restarting the system. – NonVolatile - Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.
Buttons	• **Add** - To add and save new configuration.

- **Reset** - To reset to default value for respective fields and discard all user inputs.
- **Apply** - To modify attributes for the selected entry and save the changes.
- **Delete** - To delete the selected entry.
- **Configure Target Parameter -** To access the **SNMP Target Parameter Settings** screen.

16.3.1.7 SNMP User Security Settings

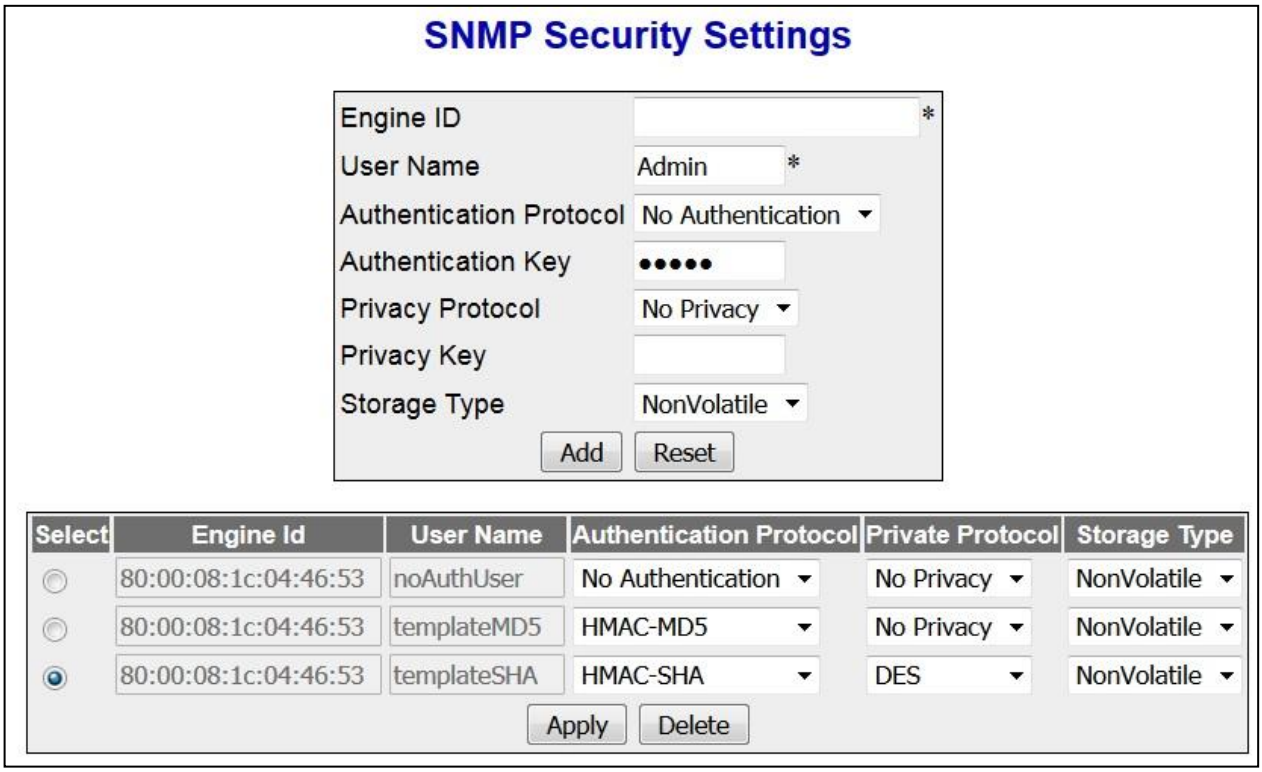


Figure 16-10 : SNMP User Security Settings

Screen Objective	This screen allows the user to create a user and configure the security parameters for that user.
Navigation	**System** > **SNMP > Agent Config. > User**
Fields	• **Engine Id** - Enter the global SNMP engine id.. The value is an octet string of maximum size 5 to 32 octets. e.g 80:00:08:1c:04:46:53 This value is used only for identification and not for addressing. This value be read from AMGnvram.txt file or from **System > NVRAM Settings > Factory Default Settings** screen while system initialization. • **User Name** - Enter the user name which is the User-based Security Model dependent security ID • **Authentication Protocol** - Select the type of authentication protocol used for authentication. The default option is **No Authentication**The list contains: – No Authentication – Sets the authentication status as no authentication required. – HMAC-MD5 – Sets the Message Digest 5 based authentication.

- HMAC-SHA – Sets the Security Hash Algorithm based authentication.

- **Authentication Key** - Enter the secret authentication key used for messages sent on behalf of this user to/from the SNMP. This value is a string of maximum size 40.

- **Privacy Protocol** - Select the type of protocol to be is used in this case. The default option is **No Privacy** The list contains:
  - No Privacy – Sets no privacy
  - DES – Sets the privacy protocol as Data Encryption Standard. This protocol provides an algorithm to encrypt PPP encapsulated packets.
  - AES – Sets the privacy protocol as Advanced Encryption Standard (AES)

- **Privacy Key** - Enter the privacy key. The messages sent on behalf of a user to/from the SNMP, can be protected from disclosure. This value is a string of maximum size 32.

- **Storage Type** - Select the required Storage type for the security settings entry. The list contains:
  - Volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system.
  - Non Volatile – Sets the storage type as permanent. Saves the configuration to the system. The Saved configuration can be viewed on restarting the system

Buttons

- **Add** - To add and save new configuration.
- **Reset** - To reset to default value for respective fields and discard all user inputs.
- **Apply** - To modify attributes for the selected entry and save the changes.
- **Delete** - To delete the selected entry.

16.3.1.8 SNMP Trap Manager Settings

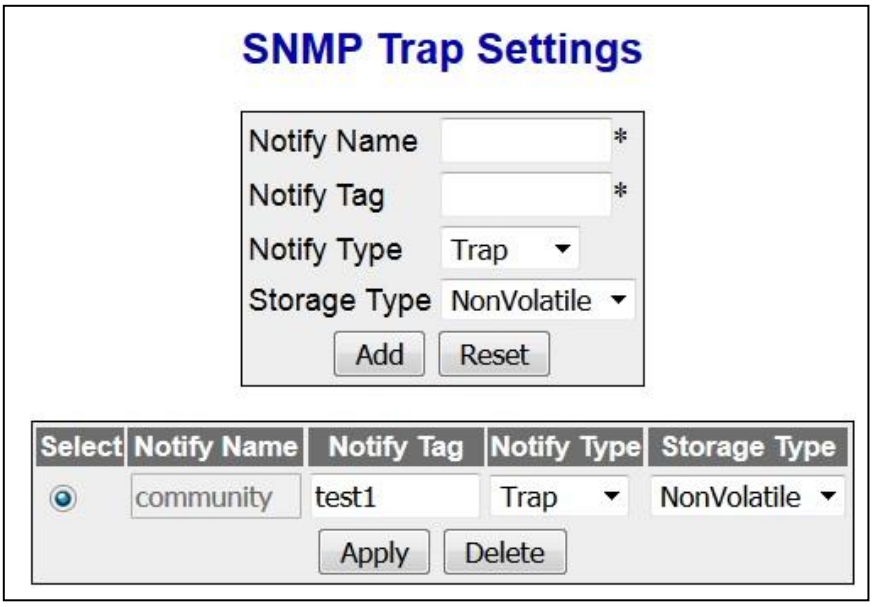


Figure 16-11 : SNMP Trap Manager Settings

Screen Objective	This screen allows the user to configure set of management targets to receive notifications
Navigation	**System** > **SNMP > Agent Config. > Trap Manager**
Fields	• **Notify Name** - Enter a unique identifier associated with the entry. The maximum size is 32. • **Notify Tag** - Enter the notification tag used to select entries in the Target Address Table. The maximum size is 32. • **Notify Type** - Select the notification type. The list contains: – Trap – Allows routers to send traps to SNMP managers. Trap is a one-way message from a network element such as a router, switch or server; to the network management system. – Inform – Allows routers / switches to send inform requests to SNMP managers • **Storage Type** - Select the required Storage type for the trap settings entry. The list contains: – Volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system. – Non Volatile – Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system.

Buttons	• **Add** - To add and save new configuration. • **Reset** - To reset to default value for respective fields and discard all user inputs. • **Apply** - To modify attributes for the selected entry and save the changes. • **Delete** - To delete the selected entry.

16.3.1.9 SNMP Filter Settings

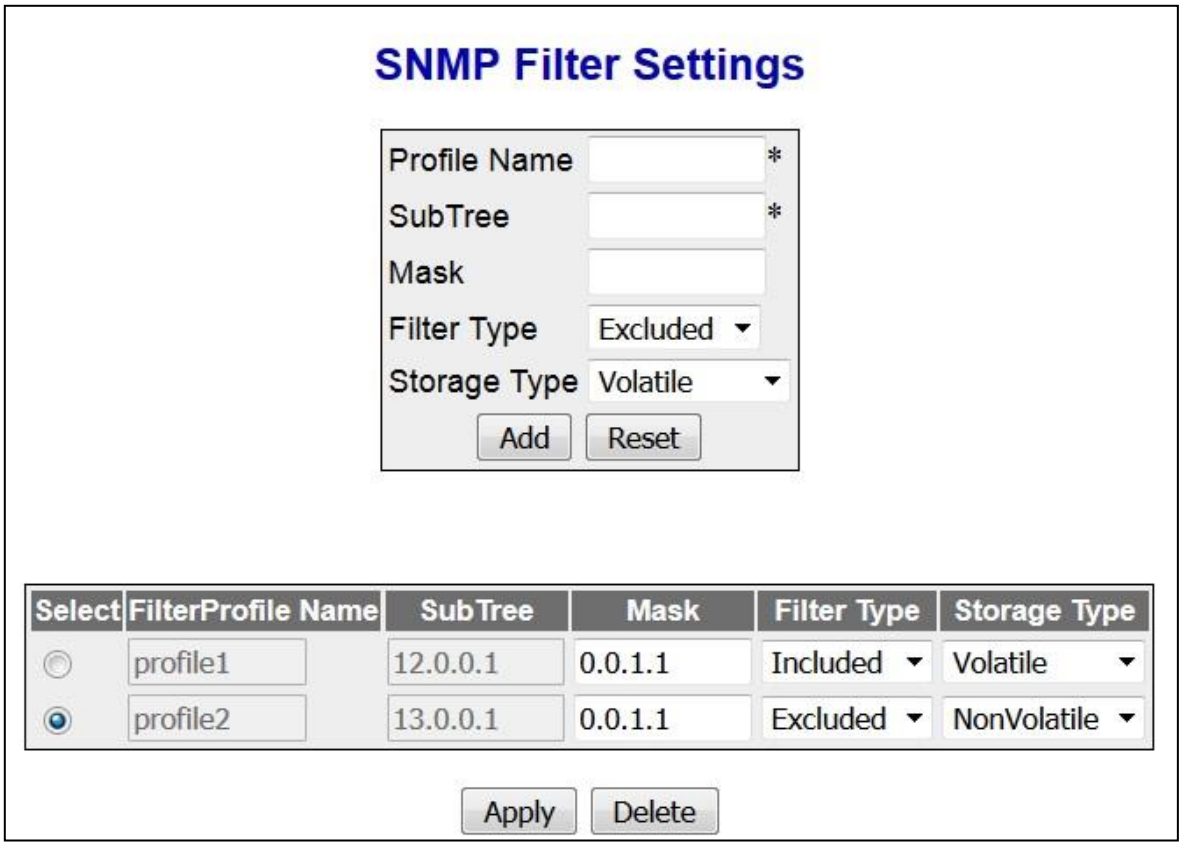


Figure 16-12 : SNMP Filter Settings

Screen Objective	This screen allows the user to configure the notification filters used to determine whether the management target should receive a particular notification. The generated notification is compared with filters associated with each management target to determine the target to which the notification is to be sent
☞	The entries in this screen can be added only if the associated filter profile entry is created through the **Filter Profile Settings** screen (**System** > **SNMP > AGENT > SNMP AGENT > TargetParameter > SNMP Target Parameter Settings** screen **>** click **Configure Filter Profile** button).
Navigation	**System** > **SNMP > Agent Config. > Filter Conf**
Fields	• **Profile Name** - Enter the filter profile name that should be used during generating notifications. This value is a string of maximum size of 32. ✎ The profile name should have been already created through SNMP Filter Profile Settings screen. • SubTree - Enter the MIB subtree that is combined with corresponding instance of mask to define a family of subtrees which are included in or excluded from the filter profile.

- **Mask** - Enter the bit mask that is combined with MIB subtree to define a family of subtrees. This is an octet string of maximum size of 16.
- **Filter Type** - Select the type of filter to be applied for the filter entry. The default option is **included**. The list contains:
  - Included – Indicates that the family of filter subtrees is defined using MIB subtree and bit mask is included in a filter.
  - Excluded - Indicates that the family of filter subtrees is defined using MIB subtree and bit mask is excluded from a filter.
- **Storage Type** - Select the storage type for the filter entry. The default option is **NonVolatile**. The list contains:
  - Volatile - Sets the storage type as temporary. Erases the configuration setting on restarting the system.
  - NonVolatile - Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system

Buttons

- **Add** - To add and save new configuration.
- **Reset** - To reset to default value for respective fields and discard all user inputs.
- **Apply** - To modify attributes for the selected entry and save the changes.
- **Delete** - To delete the selected entry.

16.4 SNMP Proxy

SNMP Proxy is used as a mediator between a SNMP manager and a SNMP Agent. It gets the request from the SNMP Agent and forwards it to the SNMP manager.

To access SNMP Proxy settings screens, click **System > SNMP > PROXY Config.**.

The SNMP Proxy related configuration related parameters are configured through the screens displayed by the following tabs:

- SNMP Proxy Settings
- SNMP MIB PROXY

By default, the **SNMP Proxy** link displays the **SNMP Proxy Settings** screen.

16.4.1 SNMP Proxy Settings

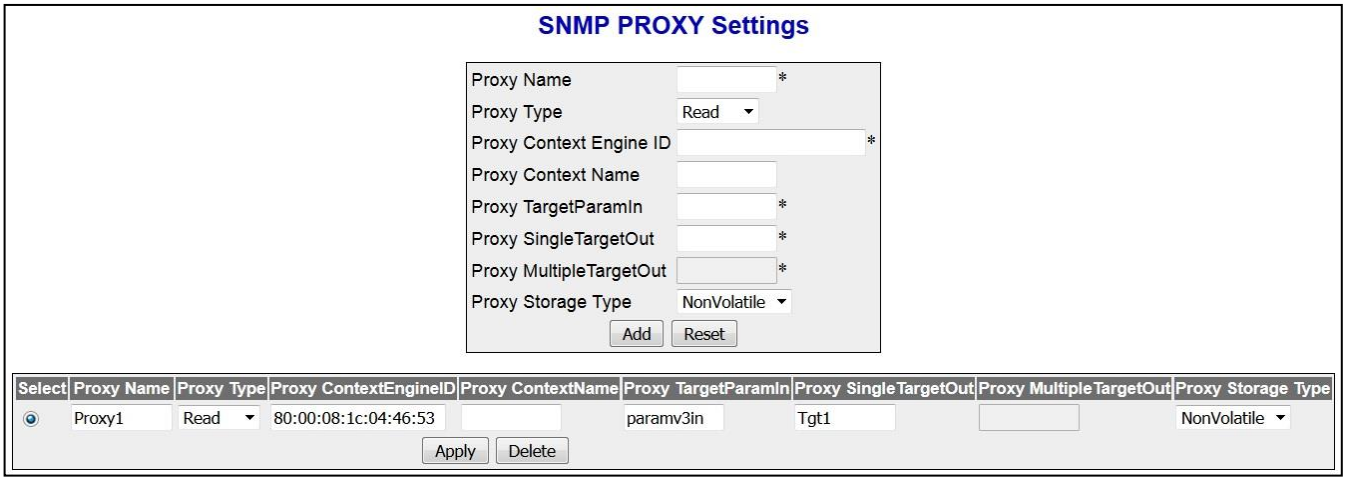


Figure 16-13 : SNMP Proxy Settings

Screen Objective	This screen allows the user to configure translation parameters for forwarding SNMP messages
Navigation	**System > SNMP > PROXY Config.. > SNMP Proxy**
Fields	• **Proxy Name** - Enter the unique proxy name that identifies an entry in the proxy table. This value is a string of maximum size of 32. • **Proxy Type** - Select the type of message to be forwarded using the translation parameters defined by proxy entry. The list contains: – Read – Read messages are forwarded to get the request from the manager. – Write – Write messages are forwarded to set configurations. – Inform – Notification messages are forwarded to the Agent. – Trap – SNMP trap messages are forwarded to the Agent • **Proxy Context Engine ID** - Enter the context engine ID of the Agent with whom the manager communicates through the proxy. • **Proxy Context Name** - Enter a unique context name for an SNMP sub Agent. This name is used to identify the corresponding sub Agent when more than one sub Agent exists. • **Proxy TargetParamIn** - Enter the SNMP version that the manager sends as request to the proxy. • **Proxy Single TargetOut** - Enter the SNMP version that the proxy uses to communicate with the Agent.

- **Proxy Multiple TargetOut** - Enter the SNMP version that the proxy uses to communicate with multiple Agents.
- **Proxy Storage Type** - Select the type of storage for the proxy. The list contains:
  - Volatile – The configuration is lost after the switch is reboot, even if the entry is saved.
  - Non-Volatile – The configuration is available even after the switch is reboot, if the entry is saved.

Buttons

- **Add** - To add and save new configuration.
- **Reset** - To reset to default value for respective fields and discard all user inputs.
- **Apply** - To modify attributes for the selected entry and save the changes.
- **Delete** - To delete the selected entry.

16.4.2 SNMP MIB Proxy Settings

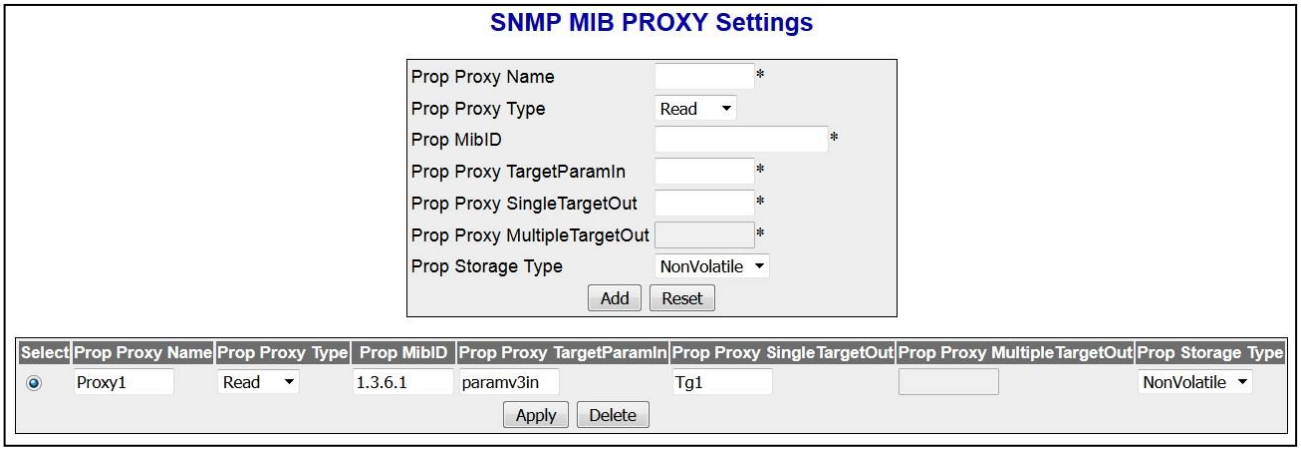


Figure 16-14 : SNMP MIB Proxy Settings

Screen Objective	This screen allows the user to configure SNMP MIB Proxy settings
Navigation	**System > SNMP > SNMP PROXY > SNMP MIB PROXY**
Fields	• **Prop Proxy Name** - Enter the unique proxy name that identifies an entry in the proxy table. This value is a string of maximum size 32. • **Prop Proxy Type** - Select the type of message to be forwarded using the translation parameters defined by proxy entry. The list contains: – Read – Read messages are forwarded to get the request from the manager. – Write – Write messages are forwarded to set configurations. – Inform – Notification messages are forwarded to the agent – Trap – SNMP trap messages are forwarded to the agent • **Prop MibID** - Enter the proprietary MIB ID which is used as the root object ID. • **Prop ProxyTargetParamIn** - Enter the SNMP version that the manager sends as request to the proxy. • **Prop ProxySingleTargetOut** - Enter the SNMP version that the proxy uses to communicate with the agent. • **Prop ProxyMultipleTargetOut** - Enter the SNMP version that the proxy uses to communicate with multiple agents. • **Prop Proxy Storage Type** - Select the type of storage for the proxy. The list contains:

	– Volatile – The configuration is lost after the switch is reboot, even if the entry is saved. – Non-Volatile – The configuration is available even after the switch is reboot, if the entry is saved.
Buttons	• **Add** - To add and save new configuration. • **Reset** - To reset to default value for respective fields and discard all user inputs. • **Apply** - To modify attributes for the selected entry and save the changes. • **Delete** - To delete the selected entry.

Chapter 16

Port Manager

Port Manager links helps to configure parameters of the ports such as MTU, Port Modes & IP specific configuration.

To access Port Manager screens, Click **Layer2 Management > Port Manager**.

Port Manager related parameters are configured through the screens displayed by the following tabs:

- Port Basic Settings
- Port Control
- Transceivers

By default, the tab **Basic Settings** displays the **Port Basic Settings** screen.

17.1 Port Manager Basic Settings

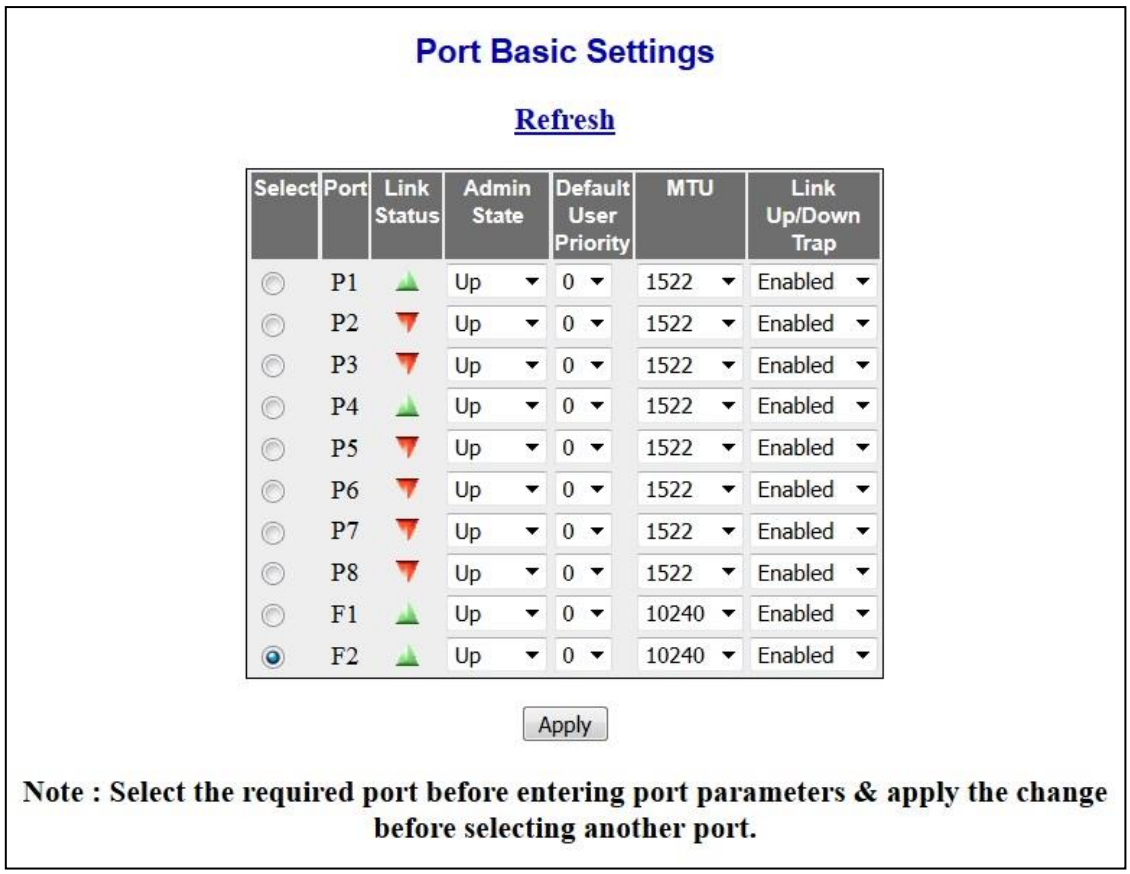


Figure 17-1 : Port Manager Basic Settings

Screen Objective	This screen allows the user to configure general information applicable for all physical ports in a switch on per port basis. You can customize all physical ports of the switch at any time
Navigation	**Layer2 Management > Port Manager > Basic Settings**
Fields	• **Select** - Click to select the port to be configured. • **Port** - Displays the port P1-P6. • **Link Status** - Displays the status of the link using graphics. The link represents a physical connection established between the switches or switch and device in a network. The graphical representation are: – **Green up arrow** – Denotes that the link is working. That is, a physical connection established for the port is active and is ready for exchange of traffic. – **Red down arrow** – Denotes that the link is not working. That is, no physical connection is established for the port or the established physical connection is not active and is a faulty one.

- **Admin State** - Select the desired state of the port. The default option is **Up.** The state changes to **Up** or **Down** state, as a result of either explicit management action or per configuration information retained by the managed system. The list contains:
  - **Up** – Allows the port to transmit/receive the traffic. The port cannot transmit/receive the traffic, if the **Link** is not working.
  - **Down** – Blocks the port from transmitting/receiving the traffic. The port will not transmit/receive the traffic, even if the **Link** is working.

- **Default User Priority** - Select the default ingress user priority for the port. The default value is **0**. The list contains values from 0 to 7. The value 0 represents the lowest priority and the value 7 represents the highest priority.

  This priority is useful only on media, such as Ethernet, that does not support native user priority.

  MTU - Select the maximum transmission unit frame size MTU for the interface. This value defines the largest PDU that can be passed by the interface without any need for fragmentation. This value is shown to the higher interface sub-layer and should not include size of the encapsulation or header added by the interface. This value represents the IP MTU over the interface, if IP is operating over the interface.

  The MTU value can be selected from 3 possible values : 1522, 2048 or 10240 bytes as follows:

Protocols	MTU in bytes
Ethernet v2, PPP, default	1522
Ethernet Jumbo Frames	2048
Ethernet Jumbo Frames	10240

  The MTU value can be changed for the interface, only whilst the Admin State of the interface is set as Down.

  The MTU value should be set as lowest of the MTU values of the member ports, while configuring for logical VLAN interfaces.

- **Link Up/Down Trap** - Select whether the linkUp / linkDown trap should be generated for the interface. The linkUp trap denotes that the communication link is available and ready for traffic flow. The linkDown trap denotes that the communication link failed and is not ready for traffic flow. The default option is **Enabled** for interfaces that do not operate on top of any other interface. Otherwise, the trap is set as **Disabled**. The list contains:
  - **Enabled** – Enables the generation of linkUp/linkDown traps for the interface.
  - **Disabled** – Disables the generation of linkUp/linkDown traps for the interface.

Buttons	**Apply** - To modify attributes and save the changes.

17.2 Port Manager Port Control

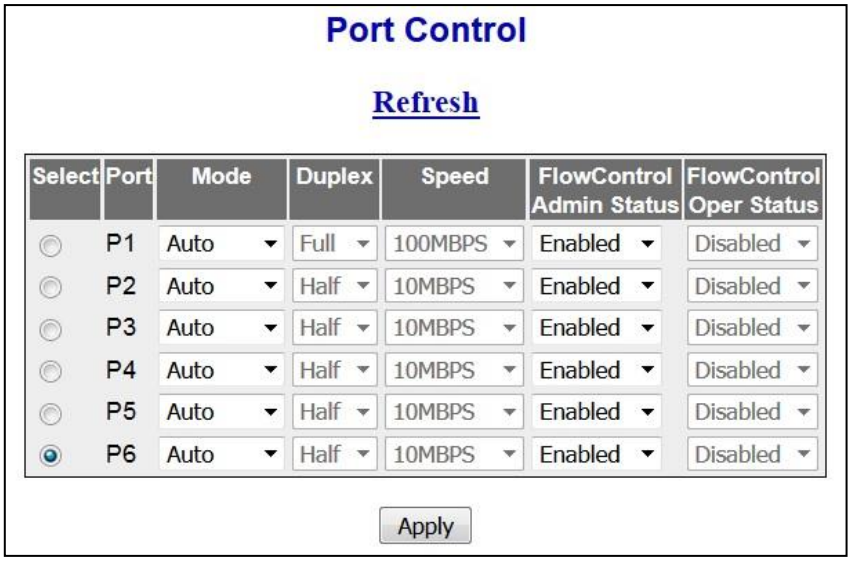


Figure 17-2 : Port Manager Port Control

Screen Objective	This screen allows the user to configure the port specific parameters such as negotiation mode of the switch
Navigation	**Layer2 Management** > **Port Manager** > **Port Control**
Fields	• **Select** - Click to select the port for which the configuration needs to be done. • **Port** - Displays the port number. • **Mode** - Select the mode of negotiation for the port. The negotiation avoids the risk of network disruption that arises from interference of dissimilar technologies with each other. The default option is **Auto**. The list contains: – **Auto** – Advertises and negotiates the parameters such as speed, duplex mode and flow control, of one port on an end of a link with other port on another end of the link to find an optimal connectivity between them. When the mode is set as Auto, the hardware senses the speed and negotiates with the port on the other end of the link for data transfer operation as full-duplex or half-duplex and about flow control. – **NoNego** – Uses the configured values for the parameters such as speed, duplex mode and flow control. This mode is used when the other switch does not have the capability to configure negotiation mode as auto and no-negotiation. When the mode is set as NoNego, the configured values for interface speed, duplex mode and flow control becomes effective. • **Duplex** - Select the duplex mode that represents the flow of data through the port. The list contains:

- **Full** – Configures interface data transfer mode as full-duplex. Ports can send and receive data at the same time.
- **Half** – Configures interface data transfer mode as half-duplex Ports can either send or receive data at that specified time.

The duplex mode can be configured, only if the negotiation **Mode** is set as **NoNego**. The duplex mode is automatically configured based on the hardware after negotiating with the peer, if the negotiation Mode is set as Auto.

- **Speed** - Select the speed of the interface.. The list contains:
  - **10 MBPS** – Sets the port speed as 10MBPS. This implies that port can transfer data at the rate of 10 Megabits per second.
  - **100 MBPS** – Sets the port speed as 100MBPS. This implies that port can transfer data at the rate of 100 Megabits per second.
  - **1 GBPS** – Sets the port speed as 1GBPS. This implies that port can transfer data at the rate of 1 Giga bits per second.

The speed can be configured, only if the negotiation **Mode** is set as **NoNego**. The speed is automatically configured based on the hardware after negotiating with the peer, if the negotiation **Mode** is set as **Auto**

- **FlowControl Admin Status** - Select the default administrative PAUSE mode for the interface. PAUSE is a flow control mechanism that is implied on full duplex Ethernet link segments. The mechanism uses MAC control frames to carry the PAUSE commands. This command is used to pause the flow of data for a time that is measured in units of quanta, where each unit is equal to 512 bit times.. The list contains:
  - **Disabled** – Disables the flow control mechanism (that is, PAUSE).
  - **Enabled** – Enables both the transmission/reception of MAC control frames used for PAUSE, to/from a remote device.

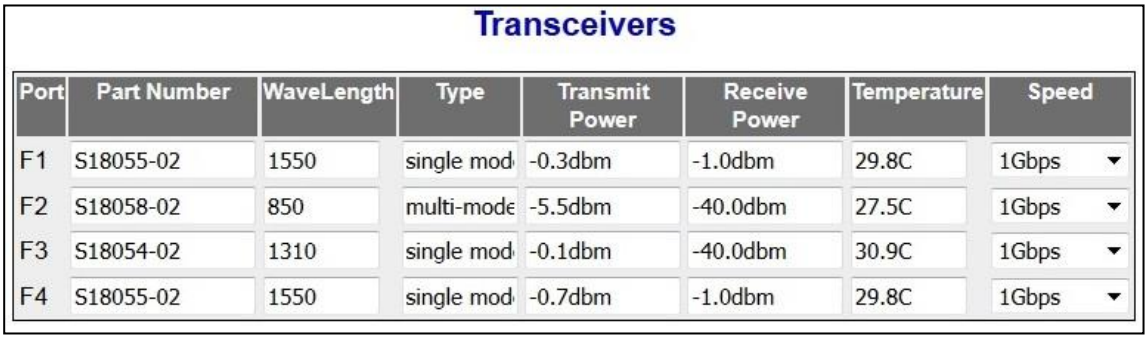
The PAUSE mode can be configured, only if the negotiation **Mode** is set as **NoNego** for the MAU attached to the interface. The PAUSE mode is automatically configured to the mode to which the interface will automatically revert once auto-negotiation is disabled, if the negotiation **Mode** is set as **Auto** for the MAU attached to the interface

This mode is applied only for the interface operating in full Duplex mode. Otherwise, the value set in this mode is ignored.

- **FlowControl Oper Status** - Displays the PAUSE mode currently used in the interface. If the negotiation **Mode** is set as **Auto** for the MAU attached to the interface, then the value is set based on the auto-negotiation function,. The list contains:
  - **Invalid** - Denotes the flow control operational status is invalid.
  - **Disabled** – Denotes that the flow control mechanism (that is, PAUSE) is disabled. This value is returned by Interfaces operating in half Duplex mode and Interfaces on which auto negotiation process is not yet completed.

	– **Transmit** – Denotes that the transmission of MAC control frames used for PAUSE, to a remote device is enabled. This value is never returned by interfaces operating at 100 Megabits per second or less. – **Receive** – Denotes that the reception of MAC control frames used for PAUSE, to a remote device is enabled. This value is never returned by interfaces operating at 100 Megabits per second or less. – **Both** – Denotes that both the transmission/reception of MAC control frames used for PAUSE, to/from a remote device is enabled.
Buttons	**Apply** - To modify attributes for the selected entry and save the changes.

17.3 Port Manager Transceivers



Transceivers

Port	Part Number	WaveLength	Type	Transmit Power	Receive Power	Temperature	Speed
F1	S18055-02	1550	single mod	-0.3dbm	-1.0dbm	29.8C	1Gbps
F2	S18058-02	850	multi-mode	-5.5dbm	-40.0dbm	27.5C	1Gbps
F3	S18054-02	1310	single mod	-0.1dbm	-40.0dbm	30.9C	1Gbps
F4	S18055-02	1550	single mod	-0.7dbm	-1.0dbm	29.8C	1Gbps

Figure 17-3 : Port Manager Tranceivers

Screen Objective

This screen displays the status of "SFP" Ports F1-Fn on the switch.

SFP stands for **S**mall **F**orm factor **P**luggable which is a standard type of pluggable (optical fibre or copper) Ethernet transceiver. Many optical fibe SFP's can provide onboard data or measurements via an internal DDM (Diagnostic Data Management) interface.

Navigation

Layer2 Management > **Port Manager** > **Transceivers**

Fields

- **Port** - Displays the port number F1-Fn. The Number (n) of SFP ports displayed is between 1 & 6 depending upon the model.
- **Part Number** - The AMG Part Number for the SFP fitted.
- **Wavelength** - The laser light wavelength in nano-metres or "0" if a copper SFP is fitted.
- **Type** - The SFP transmission mode if optical fibre SFP fitted.
  - **Single Mode** – Single mode optical fibre transmission mode
  - **Multi-Mode** – Multimode optical fibre transmission mode
  - **Copper** – Copper SFP is fitted.
- **Transmit Power** - The optical transmit power in dBm if optical SFP. Blank field if copper SFP fitted.
- **Receive Power** - The optical receive power in dBm if optical SFP. Blank field if copper SFP fitted.
- **Temperature** - The M-SES internal temperature in Degrees Celsius, measured & compensated at each SFP. Blank field if copper SFP fitted.
- **Speed** - The line speed of the SFP Ethernet data. Valid values are 10Mbps, 100Mbps, 1Gbps, Unknown.

Chapter 17

VLAN

VLAN (Virtual LAN) module logically segments the shared media LAN to form virtual workgroups. It fully utilizes the forwarding support available in the switch hardware. It redefines and optimizes the basic transparent bridging functionalities such as learning, forwarding, filtering, flooding and so on.

VLAN operates in the following modes. They are:

- **Transparent bridging** – Allows the user to connect two similar network segments to each other at the data link layer in a manner transparent to end stations, so the end stations do not participate in the bridging algorithm.
- **VLAN aware bridging** – Allows the end stations at different LAN segments to be interconnected and to communicate with each other using VLANs.

To access VLAN screens, click **Layer2 Management > VLAN**.

The VLAN related parameters are configured through the pages displayed by the following tabs:

- Global Settings
- Port Settings
- Static VLANs

By default, the tab **Basic Settings** displays the **VLAN Basic Settings** screen.

18.1 VLAN Global Settings

Figure 18-1 : VLAN Global Settings

Screen Objective	This screen allows the user to configure, for each available virtual contexts, the VLAN details that are used globally in the switch for all ports available in the switch. It allows the user to set the parameters such as VLAN type, which are fundamental for the VLAN configuration in the switch
☞	When all the VLAN type related Fields **Subnet Based On All Ports**, **MAC Based on All Ports**, **and Port Based** on All Ports are set as **Enabled**, the VLAN membership classification is done in the following order: • MAC-based VLAN classification • Subnet-based VLAN classification • Port based VLAN classification
Navigation	**Layer2 Management > VLAN > BasicSettings**
Fields	• **Select** - Click to select the context ID to configure the VLAN Basic settings for the virtual context. • **Context** - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This is a read-only field, fixed at 0. • **MAC-Address-Table Aging Time** - Enter the timeout period (in seconds) to age out the dynamically learned forwarding database entries. This timer is started once the switch identifies the MAC address. This value ranges from 10 to 1000000 seconds. The default value is **300** seconds. • **Dynamic Vlan Oper Status** - Displays the operational status of the **Dynamic VLAN** GVRP module). GVRP uses the services of GARP to propagate VLAN registration information to other VLAN aware bridges in the LAN. This information allows GVRP aware devices to dynamically establish

and update the information about the existence of the VLANs in the topology. The GVRP module registers the created VLANs with GARP and de-registers the deleted VLANs from the GARP. The default option is **Enabled**. The list contains:

- Enabled – Denotes that the GVRP module is enabled in the switch.
- Disabled – Denotes that the GVRP module is disabled in the switch.

- **Dynamic Multicast Oper Status** - Displays the operational status of the GMRP module. GMRP uses the services of GARP to propagate multicast registration information to the bridges in the LAN. This information allows GMRP aware devices to reduce the transmission of multicast traffic to the LANs, which do not have any members of that multicast group. GMRP registers and de-registers the group membership information and group service requirement information with the GARP. The default option is **Enabled**. The list contains:
  - Enabled – Denotes that the GMRP module is enabled in the switch.
  - Disabled – Denotes that the GMRP module is disabled in the switch.

- **Maximum VLAN ID** - Displays the largest valid VLAN / VFI ID accepted in the system.
  - **<**vlan –id> - This is a unique value that represents the specific VLAN. This value ranges from 1 to 4093

    The VLAN ID cannot be configured greater than the value displayed in the field.

- **Maximum Supported VLANs** - Displays the maximum number of VLANs the switch can support. This value ranges from 1 to 256

- **Number of VLANs in the System** - Displays the total number of VLANs currently active in the device. By default, Vlan 1 is active in the sytem and hence this value is set as 1.

Buttons

- **Apply** - To modify attributes for the selected entry and save the changes.
- **Configure VLAN Trace Options -** To access to the **VLAN Traces** screen

18.2 VLAN Port Settings

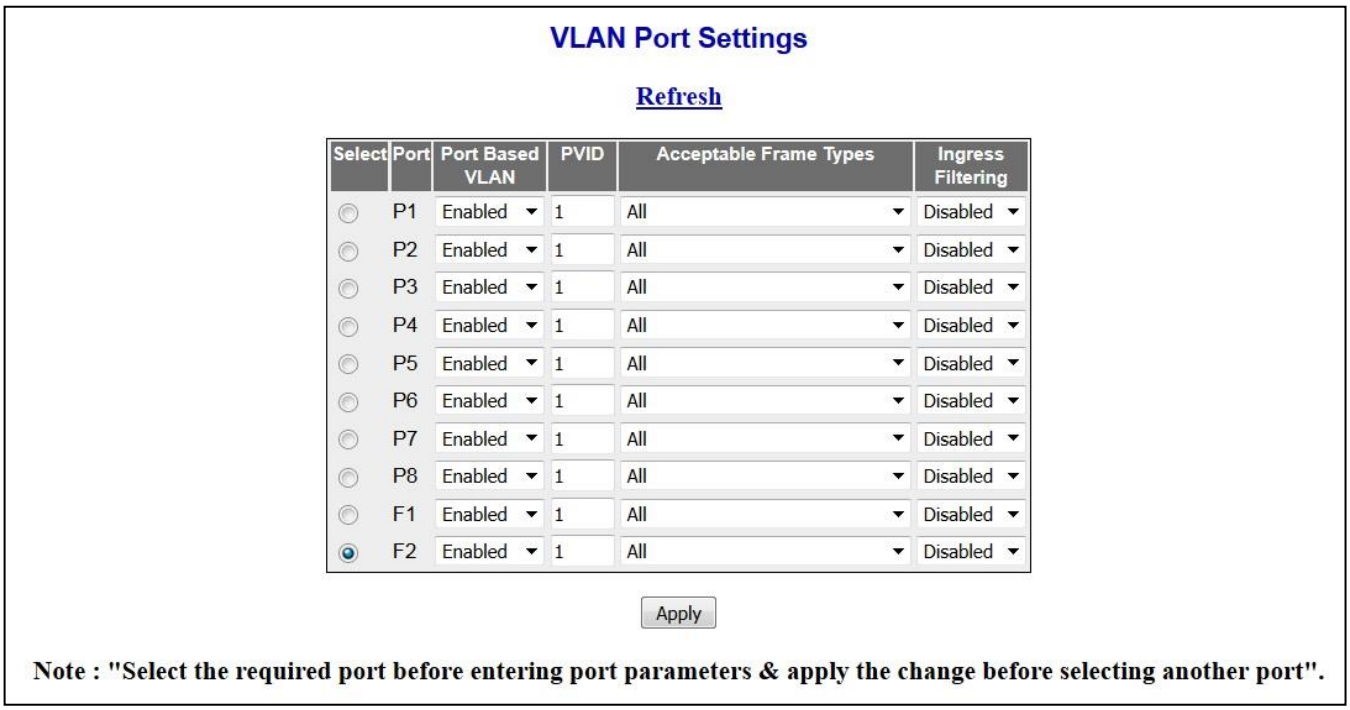


Figure 18-2 : VLAN Port Settings

Screen Objective	This screen allows the user to configure VLAN details such as VLAN acceptable Frame Types, for the physical ports available in the device
Navigation	**Layer2 Management > VLAN > PortSettings**
Fields	• **Select** - Click to select the port to configure. • **Port** - Displays the port number. P1-P6 • **Port Based VLAN** - Select whether the VLAN membership classification is supported by the port. VLAN membership classification is done for all untagged and priority-tagged frames based on the port. The list contains: – **Enabled** – Enables port based VLAN classification in the port. – **Disabled** – Disables port based VLAN classification in the port. This field can be configured independently without depending on the VLAN type configuration done globally in the device. That is, this field does not depend upon the value set in the field Port Based on All Ports. • **PVID** - Displays the PVID, which represents the VLAN ID assigned to untagged frames or priority-tagged frames received on the port. The PVID is

used for port based VLAN type membership classification. The default VLAN ID (that is, 1) is set as the PVID. This value ranges from 1 to 4094.

- **Acceptable Frame Types** - Select the type of VLAN dependent BPDU frames to be accepted by the port during the VLAN membership configuration. The default option is **All**. The list contains:
  - **All** – Accepts tagged, untagged and priority tagged frames received on the port and subjects the frames to **Ingress Filtering** setting.
  - **Tagged** – Accepts only the tagged frames received on the port. Rejects untagged or priority tagged frames received on the port.
  - **UnTagged and Priority Tagged** – Accepts only the untagged or priority tagged frames received on the port. Rejects tagged frames received on the port.

  This field does not affect VLAN independent BPDU frames such as GVRP BPDU and STP BPDU. It affects only the VLAN dependent BPDU frames such as GMRP BPDU.

  The frame type is always set as UnTagged and Priority Tagged, if the Bridge Port Type is set as CustomerNwPort.

- **Ingress Filtering** - Select whether the filtering should be applied for the incoming frames received on the port. The default option is **Disabled**. The list contains:
  - **Enabled** – Accepts only the incoming frames of the VLANs that have this port in its member list.
  - **Disabled** – Accepts all incoming frames received on the port.

  This field does not affect VLAN independent BPDU frames such as GVRP BPDU and STP BPDU. It affects only the VLAN dependent BPDU frames such as GMRP BPDU.

  The ingress filtering cannot be disabled for port whose Switch Port Mode is set as host or promiscuous.

Buttons	**Apply** - To modify attributes for the selected entry and save the changes.

18.3 VLAN Static Configuration

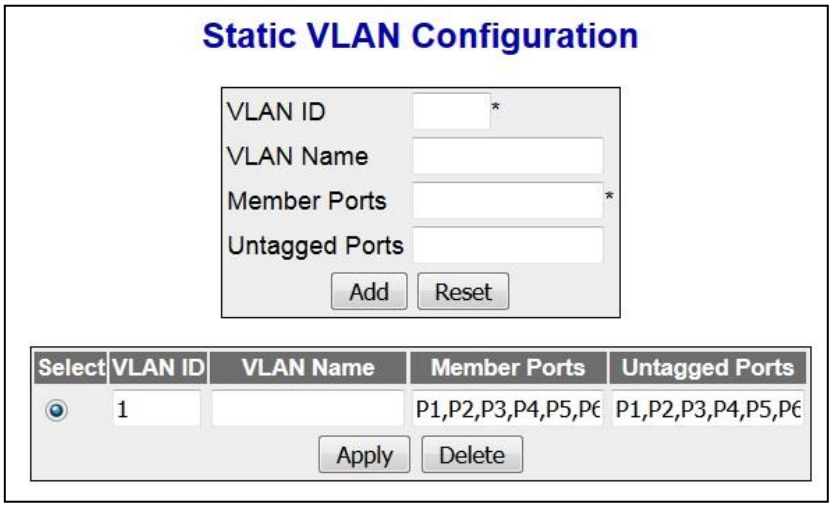


Figure 18-3 : Static VLAN Configuration

Screen Objective

This screen allows the user to create / delete VLANs in the switch and statically configure details such as member port, for the VLANs in the switch. These static configuration details are permanent and can be restored after the switch is reset.

> The default VLAN ID (Management ID) cannot be deleted. The default Management VLAN ID is 1, but this can be changed if required in the "System Information" Page.

Navigation

Layer2 Management > VLAN > Static VLANs

Fields

- **Select** - Click to select the vlan id for which the configuration needs to be modified or deleted.
- **VLAN ID** - Enter the VLAN ID that uniquely identifies a specific VLAN. This value ranges from 1 to 4094.
- **VLAN Name** - Enter an administratively assigned string, which is used to identify the VLAN. This vlaue is a string of maximum size 32.
- **Member Ports** - Enter a port or a set of ports, which need to be part of the VLAN identified by the VLAN ID. Use comma as a separator between the ports while configuring a list of ports. This list includes both tagged and untagged members of the VLAN.
- **Untagged Ports** - Enter port or set of ports, which should transmit egress packets for the VLAN as untagged packets. Use comma as a separator between the ports while configuring a list of ports. Ports which are attached to VLAN-unaware devices should be configured as untagged-ports for a

given VLAN. The untagged ports list should be a sub-set of the **VLAN Member Ports**.

- The port can be configured as a untagged port, only if the Switch Port Mode of the port is not set as trunk.
- The ports configured as untagged ports should be a subset of Member Ports

Buttons

- **Add** - To add and save new configuration.
- **Reset** - To reset to default value for respective fields and discard all user inputs.
- **Apply** - To modify attributes for the selected entry and save the changes.
- **Delete** - To delete the selected entry.

Chapter 18

Address Tables

Address Tables

Traffic forwarding is based on dynamic address table information. Address tables contain information about MAC addresses those are dynamically learned on the device. As the name implies, this dynamic address database changes based on incoming traffic into the device. Each entry in dynamic MAC address table consists of VLAN Id, MAC Address and interface information.

Dynamic MAC entries get aged based on ageing interval configured on the device. AMG9IM2x/9HM2x Product Series provides web interface to view MAC address table and also provides web interface to configure MAC table aging interval.

To access the MAC address table screens, click :

Layer2 Management > Address Tables

MAC address related parameters are configured through the screens displayed by the following tabs:

- MAC Table
- Static Unicast Entries
- Static Multicast Entries

By default, the tab Address Tables displays the **MAC table** screen.

19.1 Address Tables MAC Table

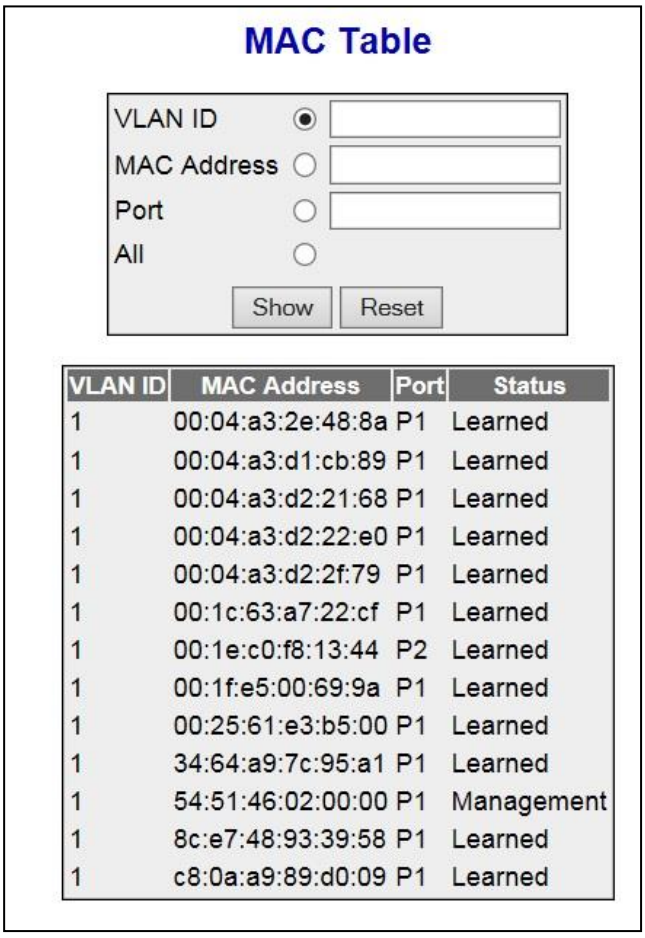


Figure 19-1 : Address Tables MAC Table : VLAN ID

Screen Objective	This screen allows the user to view the MAC tables created in the system
Navigation	**Layer2 Management > Address Tables > MAC Table**
Fields	• **VLAN ID** - View by VLAN ID. • **MAC Address** - View by MAC Address. • **VLAN ID** - View by Port (1-6) • **VLAN ID** - View All MAC Address's.
Buttons	• **Show** - To display MAC Address table for the selected range. • **Reset -** To clear the entry fields.

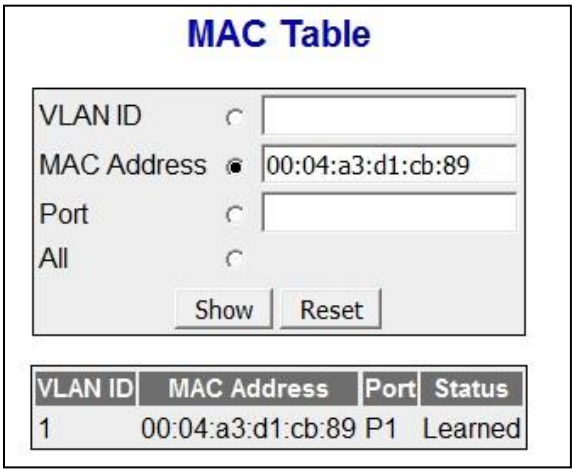


Figure 19-2 : Address Tables MAC Table : MAC address

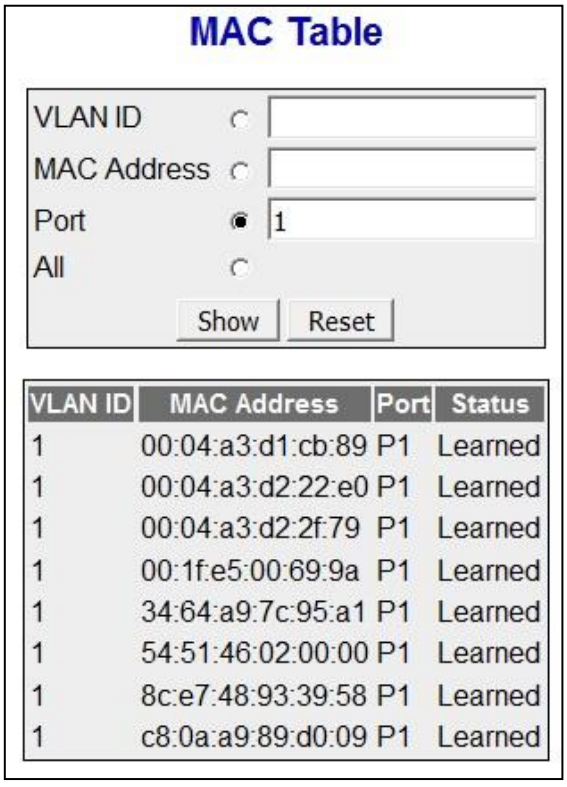


Figure 19-3 : Address Tables MAC Table : Port

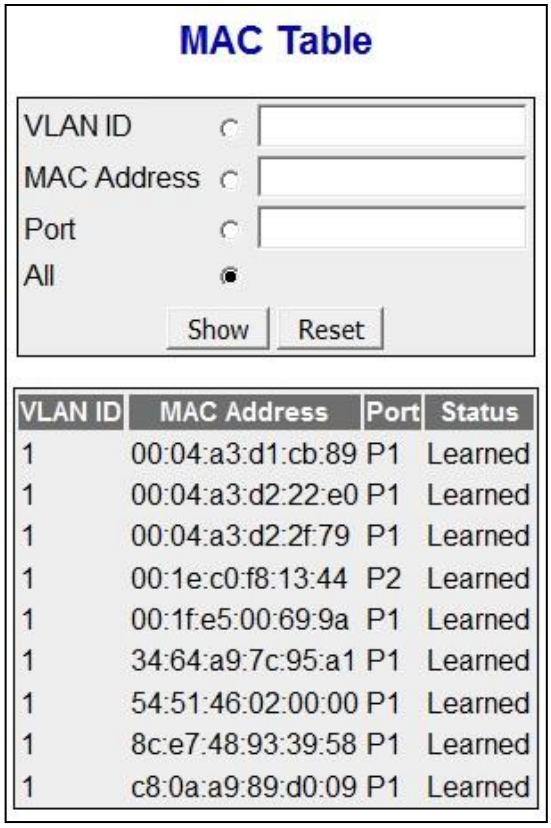


Figure 19-4 : Address Tables MAC Table : All

19.2 Address Tables Static Unicast Entries

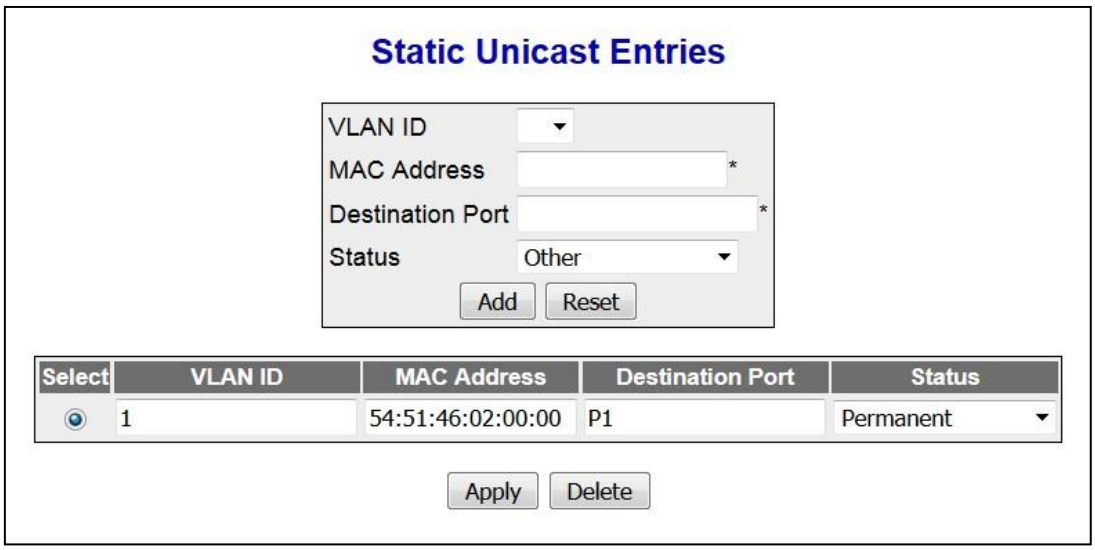


Figure 19-5 : Address Tables Static Unicast Entries

Screen Objective	This screen allows the user to view the Static Unicast Address's created in the system
Navigation	**Layer2 Management > Address Tables > Static Unicast Entries**
Fields	• **VLAN ID** - Select the VLAN ID. • **MAC Address** - Enter the Static Unicast MAC Address. • **Destination Port** - Enter the required Port (P1-P6) • **Status** - Select the ageing / expiry mode of the Static Unicast entrry. The list contains: – **Permanent** – never expires – **DeleteOnReset** - expires when unit is reset – **DeleteOnTimeout** - expires when timer expires
Buttons	• **Add** - To enter the Static Unicast MAC Address • **Reset -** To clear the entry fields. • **Select** - Radio Button to select the entry to modify • **Apply -** Apply the change to the selected entry • **Delete -** Deletes the selected entry

19.3 Address Tables Static Multicast Entries

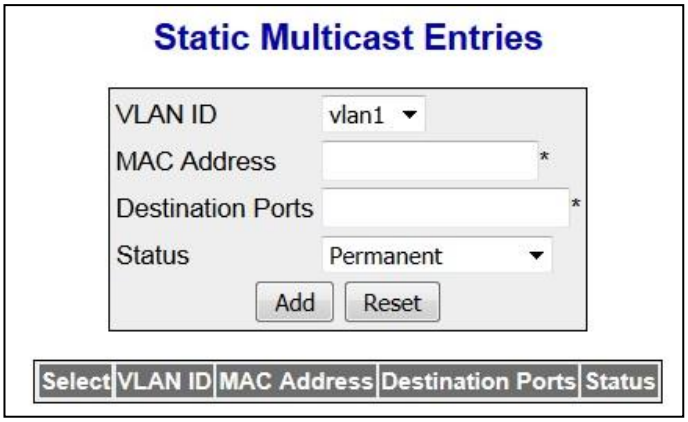


Figure 19-6 : Address Tables Static Multicast Entries

Screen Objective	This screen allows the user to view the Static Multicast Address's created in the system
Navigation	**Layer2 Management > Address Tables > Static Multicast Entries**
Fields	• **VLAN ID** - Select the VLAN ID. • **MAC Address** - Enter the Static Unicast MAC Address. • **Destination Ports** - Enter the required Port (P1-P6) • **Status** - Select the ageing / expiry mode of the Static Multicast entrry. The list contains: – **Permanent** – never expires – **DeleteOnReset** - expires when unit is reset – **DeleteOnTimeout** - expires when timer expires
Buttons	• **Add** - To enter the Static Multicast MAC Address • **Reset -** To clear the entry fields. • **Select** - Radio Button to select the entry to modify • **Apply -** Apply the change to the selected entry • **Delete -** Deletes the selected entry

Chapter 19

MSTP

MSTP (Multiple Spanning Tree Protocol) is used to configure spanning tree on per VLAN basis or multiple VLANs per spanning tree. It allows the user to build several MST over VLAN trunks, and group or associate VLANs to spanning tree instances, so the topology of one instance is independent of the other instance. It provides multiple forwarding paths for data traffic and enables load balancing. It improves the overall network fault tolerance, as failure in one instance does not affect the other instances.

The MSTP provides an optional capability for:

- High availability
- Executing multiple instances of the protocol
- Provider bridging

To access MSTP screens, click **Layer2 Management > MSTP.**

The MSTP related parameters are configured through the screens displayed by the following tabs:

- Global Configuration
- Timers
- Port Configuration
- VLAN Mapping
- Port Settings
- CIST Port Status
- Bridge Priority

By default, the tab **Global Configuration** displays the **Global Configuration** screen.

20.1 MSTP Global Configuration

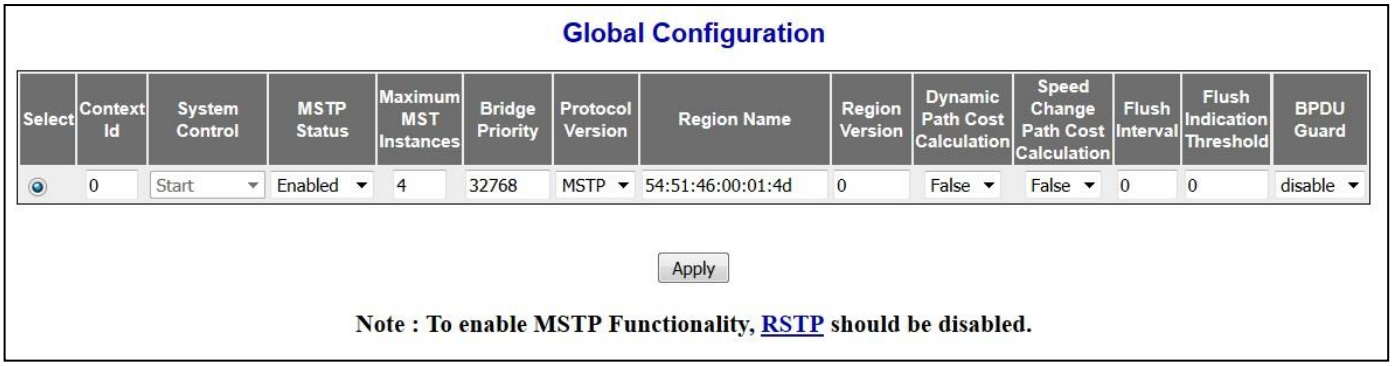


Figure 20-1 : MSTP Global Configuration

Screen Objective

This screen allows the user to configure, for each available virtual contexts, the MST module parameters that are used globally in the switch for all ports

To enable MSTP, the following should be disabled in the selected context.

- RSTP
- PVRST

Navigation

Layer2 Management > MSTP > Global Configuration

Fields

- **Select** - Click to select the context for which the configuration needs to be done.
- **Context Id** - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This is a read-only field, fixed at 0.
- **System Control** - Select the administrative shutdown status requested by management for the MSTP module. The default option is **Start**. The list contains:
  - **Start** – Specifies that MSTP is active in the device on all ports.
  - **Shutdown** – Specifies that MSTP is shutdown in the device on all ports and all allocated memory is released.

  The administrative status can be set as Shutdown, only if the MSTP Status is set as Disabled. The status can be set as Start, only if the RSTP System Control is set as Shutdown using the **Layer2 Management > RSTP > Global Configuration** screen.

  MSTP System Control cannot be shutdown if MSTP status is enabled.
- **MSTP Status** - Select the administrative status requested by management for the MST feature. MSTP is used to configure spanning tree on per VLAN

basis or multiple VLANs per spanning tree. It provides multiple forwarding paths for data traffic and enables load balancing. The default option is **Enabled** for the default context and Disabled for the other contexts. The list contains:

- **Enabled** – Enables MST in the device on all ports.
- **Disabled** – Disables MST in the device on all ports.

To enable MSTP globally in the switch, the MSTP **System Control** status should be set as Start.

All the **Fields** in this screen (except the **System Control**) are greyed out and cannot be configured, once the MSTP status is set as Disabled.

- **Maximum MST Instances** - Enter the maximum number of spanning trees to be allowed in the switch. This value represents the maximum number of active MSTIs that can be created. This allows the user to limit the number of spanning tree instances to be allowed in the switch. This value ranges from 1 to 4. The default value is **4**.

  The maximum available number of instances is 4

- **Bridge Priority** - Enter the priority value that is assigned to the switch. This value is used during the election of CIST root, CIST regional root and IST root. This value ranges from 0 to 61440. The default value is **32768**.The values set for Bridge Priority must be in steps of 4096.

- **Protocol Version** - Select the version of STP in which the switch is currently running. This allows the user to set the type of STP to be used by the switch to form loop-free topology. The default option is **MSTP**. The list contains:
  - **STP** – Sets the version as spanning tree protocol specified in IEEE 802.1D.
  - **RSTP** – Sets the version as Rapid spanning tree protocol specified in IEEE 802.1w.
  - **MSTP** – Sets the version as multiple spanning tree protocol specified in IEEE 802.1s.

  The Fields Region Name and Region Version are greyed out and cannot be configured, if the protocol version is set as STP or RSTP.

- **Region Name** - Enter the name for the region's configuration to identify the specific MST region. Each MST region contains multiple spanning tree instances and runs special instance of spanning tree known as IST to disseminate STP topology information for other STP instances. The default value is same as that of the Switch Base MAC Address configured in the **Factory Default Settings** screen. This value is an octet string of maximum size 32.

  This field can be configured only if the protocol version is selected as MSTP.

- **Region Version** - Enter the version that represents the specific MST region. The default value is **0**.This value ranges from 0 to 65535.

This field can be configured only if the protocol version is selected as MSTP.

- **Dynamic Path Cost Calculation** - Select whether the dynamic path cost calculation is allowed or not..The path cost represents the distance between the root port and designated port. The path cost is based on a guideline established as part of 802.1d. The path cost is dynamically calculated using port speed, when the operational status of the port changes from down to up.or link speed at the time of port creation The default option is **False**. The list contains:
  - **True** – Dynamically calculates path cost based on the speed of the ports whose **Admin State** is set as **Up** at that time. The path cost is not changed based on the operational status of the ports, once calculated.
  - **False** – Dynamically calculates path cost based on the link speed at the time of port creation

  The manually assigned path cost is used irrespective of the status (**True** or **False**) of the dynamic path cost calculation.

- **Speed Change Path Cost Calculation** - Select whether the speed change path cost calculation is allowed or not. The speed change path cost is to be calculated for ports whose speed changes dynamicallyThis feature is mainly used for LA (Link Aggregated) ports whose speed changes due to the addition and deletion of ports from the port channel. The default option is **False**. The list contains::
  - **True** – Specifies that path cost is dynamically calculated for ports based on their speed at that time. The path cost is calculated, if the speed of the port changes.
  - **False** – Specifies that path cost is not dynamically calculated for ports based on their speed at that time.

  The manually assigned path cost is used irrespective of the status (**True** or **False**) of the path cost calculation, if Path Cost for the port is manually assigned.

- **Flush Interval** - Enter the value that controls the number of flush indications invoked from spanning-tree module per instance basis. This value ranges from 0 to 500 centi-seconds. The default value is 0.

  If the flush interval timer is set to zero, port and instance based flushing occurs(default functionality).

  If it is set to non-zero, instance based flushing occurs (dependent on the flush-indication-threshold value).

- **Flush Indication Threshold** - Enter the number of flush indications to go before the flush-interval timer method triggers. This value ranges from 0 to 65535. The default value is **0**.

  The flush indication threshold value can be configured only when flush interval value is other than default value.

  When flush indication threshold is default value and flush interval is non-default value, instance based flushing occurs during the first flush indication trigger.

When the flush indication threshold value is non-default(x) and flush-interval value is non-default, port & instance based flushing is triggered until the threshold(x) is reached. Once the threshold is reached, instance based flushing is triggered & timer starts.

- **BPDU Gaurd** - Select the administrative status for the BPDU guard feature in the port.This feature configures BPDU guard globally in MSTP and this global BPDU is applicable if and only if no port specific BPDU Guard is configured. The default option is **Disable.** The list contains:
  - **Enabled** - Enables BPDU Guard feature on edge ports globally and. moves the port to disabled discarding state when BPDU is received on the edge ports
  - **Disabled** - Disables BPDU Guard feature on edge ports globally.

Buttons

- **Apply** - To modify attributes for the selected entry and save the changes.

20.2 MSTP Timers

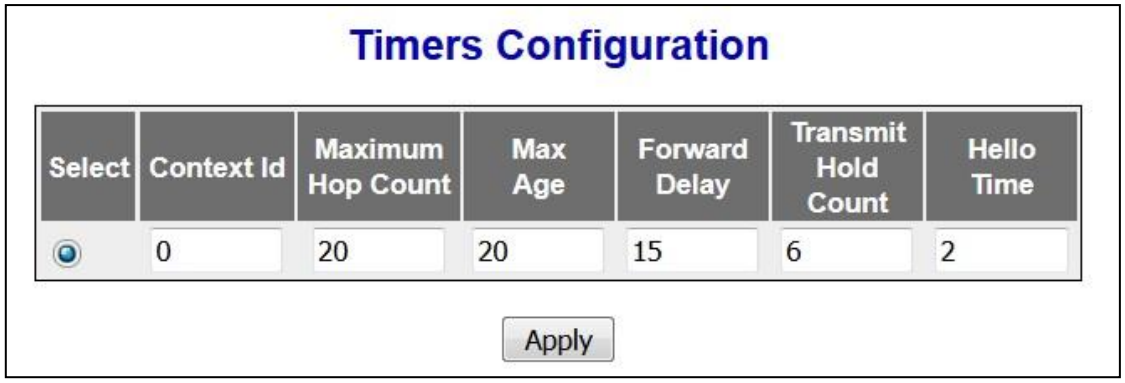


Figure 20-2 : MSTP Timers Configuration

Screen Objective	This screen allows the user to configure the timers used in MSTP protocol for controlling the transmission of BPDUs during the computation of loop free topology. This configuration is applied globally in the switch on all ports
☞	This screen displays the default configuration details only for the context for which the MSTP **System Control** status is set as **Start.** For the contexts for which MSTP is shutdown, it displays the value as 0 for all fields**.**
Navigation	**Layer2 Management** > **MSTP** > **Timers**
Fields	• **Select** - Click to select the context for which the configuration needs to be applied. • **Context Id** - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This is a read-only field, fixed at 0. • **Maximum Hop Count** - Enter the maximum hop count value. that represents the maximum number of switches that a packet can cross before it is dropped. This value is used by the switch to avoid infinite looping of the packets, if it is selected as the root switch in the topology. This value ranges from 6 to 40. The default value is **20**. The root switch always transmits a BPDU with the maximum hop count value. The receiving switch decrements the value by one and propagates the BPDU with modified hop count value. The BPDU is discarded and the information held is aged out, when the count reaches 0. • **Max Age** - Enter the amount of time a port waits for STP/RSTP information.. This value is used by MSTP while interacting with STP/RSTP domains on the boundary ports. This value ranges from 6 to 40 seconds. The default value is **20** seconds. ✎ The maximum age should be lesser than or equal to 2*(Forward Delay - 1.0) and should be greater than or equal to 2*(HelloTime + 1.0)

- **Forward Delay** - Enter the number of seconds a port waits before changing from the learning/listening state to the forwarding state. This value ranges from 4 to 30 seconds. The default value is **15** seconds
- **Transmit Hold Count** - Enter the value used by the port transmit state machine to limit the maximum transmission rate i.ethe number of packets that can be sent in a given intervalThis value is configured to avoid flooding. Port transmit state machine uses this value to limit the maximum transmission rate. This value ranges from 1 to 10. The default value is **6**.
- **Hello Time** - Enter the amount of time between the transmission of configuration bridge PDUs by this node. . This value can be either 1 or 2 seconds. The default value is **2**.

Buttons	**Apply** - To modify attributes for the selected entry and save the changes.

20.3 MSTP Port Configuration

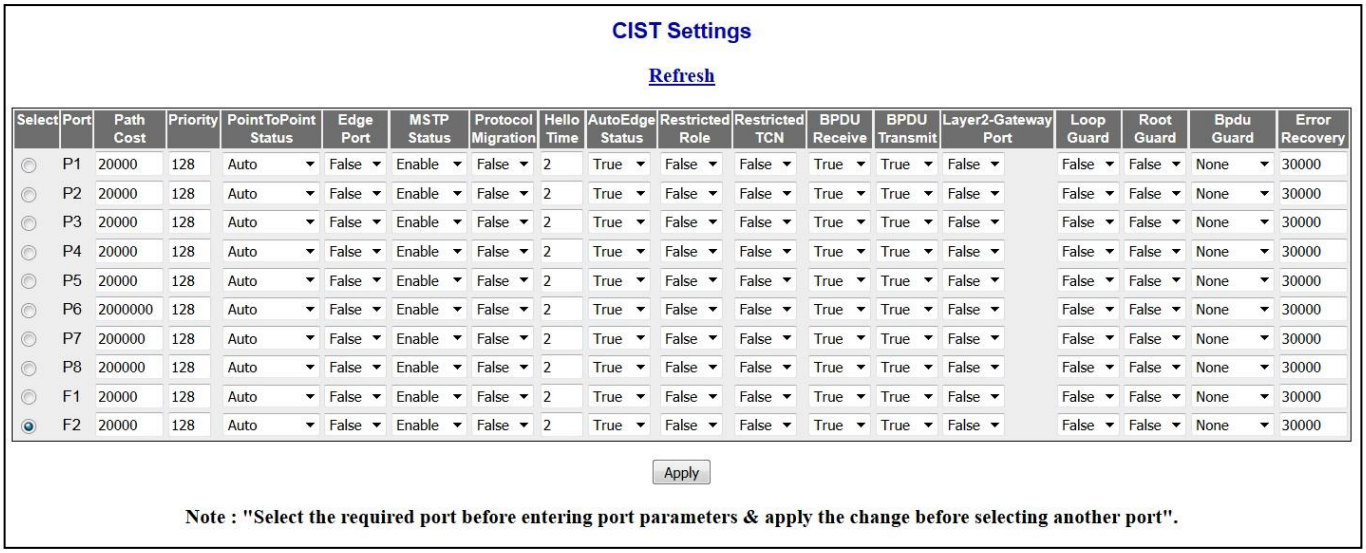


Figure 20-3 : MSTP Port Configuration

Screen Objective

This screen allows the user to configure the port information for CIST, which spans across the entire topology irrespective of MST and SST regions. CIST is a single common/active topology consisting of all switches in the topology.

The parameters in the screen are not populated with the values (the screen is blank), if the MSTP **System Control** status is set as **Shutdown** for the context selected using the **Context Selection** screen.

Navigation

Layer2 Management > **MSTP** > **Port Configuration**

Fields

- **Select** - Click to select the port for which the configuration needs to be applied.
- **Port** - Displays the port number.
- **Path Cost** - Enter the value that contributes to the path cost of paths towards the CIST Root which includes this port. The paths' path cost is used during calculation of shortest path to reach the CIST root. The path cost represents the distance between the root port and designated port. This value ranges from 1 to 200000000. The default value is **200000** for all physical ports and **199999** for port channels.

  The default value is used as the path cost, if this field is not configured and the **Dynamic Path Cost Calculation** and **Speed Change Path Cost Calculation** are set as False. The dynamically calculated path cost is used if the path cost is not manually configured and one of these **Fields** is set as True.

  The configured value is used as the path cost irrespective of the status (True or False) of the **Dynamic Path Cost Calculation** and **Speed Change Path Cost Calculation.**

- **Priority** - Enter the priority value that is assigned to the port. This value is used during the role selection process. The four most significant bits of the Port Identifier of the Spanning Tree instance can be modified by setting the Cist Port Priority value. The values that are set for Port Priority must be in steps of 16. This value ranges from 0 to 240. The default value is **128**.

- **Point-to-Point Status** - Select the point-to-point status of the LAN segment attached to the port. The default option is **Auto**. The list contains:
  - **ForceTrue** – Specifies that port is connected to a point-to-point link.
  - **ForceFalse** – Specifies that port is having a shared media connection.
  - **Auto** – Specifies that the ports as having a shared media connection or a point-point link based on the prevailing conditions.

  Port is considered to have a point-to-point link if,

  - It is an aggregator and all of its members can be aggregated.
  - The MAC entity is configured for full **Duplex** operation, either manually or through auto negotiation process (that is, negotiation **Mode** is set as **Auto**).

- **Edge Port** - Select the administrative value of the Edge Port parameter. The default option is **False**. The list contains:
  - **True** – Sets the port as an edge port (the **Port State** is immediately set as **forwarding**). It is connected directly to a single end station. It allows MSTP to converge faster and does not wait to receive BPDUs.
  - **False** – Sets the port as a non-Edge port (the spanning tree process is performed using the MSTP). It is connected to a routing device such as switch.

  The value of the Edge Port parameter depends on the option selected in the field Auto Edge Status. The value of the Edge Port parameter is automatically updated, if the Auto Edge Status is set as **True**.

- **MSTP Status** - Select the MSTP status of the port for all spanning tree instances. This value will override the port's status in the MSTI contexts. The default option is **Enable**. The list contains:
  - **Enable** – Enables MST in the port. MAC frames are forwarded and their source addresses are learnt.
  - **Disable** – Disables MST in the ports. MAC frames are not forwarded and their source addresses are not learnt.

- **Protocol Migration** - Select the protocol migration state of the port.This is used to control the protocol migration mechanism that enables the module to interoperate with legacy 802.1D switches. The default option is **False**. The list contains:
  - **True** – Specifies that the port transmits BPDUs based on the spanning tree protocol supported by the receiving switch. The port is forced to transmit MSTP BPDUs without instance information.
  - **False** – Specifies that the port does not perform protocol migration mechanism. The port always transmits the standard MSTP BPDUs.

The protocol migration is greyed out and cannot be configured, if the MSTP Status is set as Disable.

- **Hello Time** - Enter the amount of time between between the transmission of Configuration bridge PDUs by this node in units of hundredths of a second. This value can be either 1 or 2 seconds. The default value is **2** seconds.
- **Auto Edge Status** - Select whether the Edge Port parameter of the port is detected automatically or configured manually. The default option is **True**. The list contains:
  - **True** – Specifies that detection of port as Edge Port happens automatically. The port is set as edge port, if no BPDU is received on the port. The port is set as non-edge port, if any BPDU is received by that port. This overrides the value set in the field **Edge Port**, based on the reception of BPDU.
  - **False** – Specifies that the auto edge feature is disabled and the manually configured value for the Edge Port parameter is used.
- **Restricted Role** - Select whether the selection of port **Role** as root can be blocked during the role Selection process. This feature allows the user to block switches external to a core region of the network from influencing the spanning tree active topology. The default option is **False**. The list contains:
  - **True** – Blocks the port from being selected as root port for the CIST or any MSTI, even if it has the best spanning tree priority vector. It is selected as an alternate port after the root port is selected.

    The blocking of port from being selected as a root port may cause lack of spanning tree connectivity.
  - **False** – Includes all available ports of the topology, in the root selection process to select the root for CIST or any MSTI.
- **Restricted TCN** - Select the status of transmission of the received topology change notifications and topology changes to the other ports in the network. This feature allows the user to block switches external to a core region of the network from causing address flushing in the region. The default option is **False**. The list contains:
  - **True** – Blocks the port from propagating the received topology change notifications and topology changes to other ports.

    The blocking of port may cause temporary loss of connectivity after changes in a spanning tree active topology as a result of persistent incorrectly learnt station location information.
  - **False** – Allows the port to propagate the received topology change notifications and topology changes to other ports.
- **BPDU Receive** - Select the processing status of the received MSTP BPDUs. The default option is **True**. The list contains:
  - **True** – Normally processes the MSTP BPDUs received on the port.
  - **False** – Discards the MSTP BPDUs received on the port.

- **BPDU Transmit** - Select the BPDU transmission status of the port. The default option is **True**. The list contains:
  - **True** – Specifies that MSTP BPDUs are transmitted from the port.
  - **False** – Specifies that MSTP BPDUs transmission is blocked from the port.

  This field should be set as False, for ports to be configured as Layer-2 Gateway Port.

- **Layer2-Gateway Port** - Select whether the port acts as a normal port or as a L2GP.The default option is **false**. The list contains:
  - **True** – Specifies that the port operates as a Layer2 Gateway Port.
  - **False** – Specifies that the port operates as a normal Port.

  BPDU Transmit , Restricted Role and **Restricted TCN** should be set as False, before configuring the port as a Layer2 gateway port.

  L2GP should not be enabled on ports whose Bridge Port Type is set as PIPs or CBPs, as the effect is unknown.

  L2GP operates similar to that of the normal port operation but pretends to continuously receive BPDUs when **Admin State** is set as **Up**

  L2GP cannot be enabled on ports with SISP enabled interfaces. The Port State of the L2GP is always set as discarding.

- **Loop Guard** - Select the status of loop guard.. The Loop Guarddoes age out the information even if the peer does not send information. If the port continues to receive information through BPDUs, the operation on this port will be normal. This is useful when the neighbor bridge is faulty, that is, the bridge cannot send BPDUs but continues to send data traffic. The default option is **False**. The list contains:
  - **True** – Enables the loop guard in the port.
  - **False** – Disables the loop guard in the port.

- **Root Gaurd** - Select the administrative status for the root guard feature in the port. This feature when enabled causes the Port not to be selected as Root Port for the CIST or any MSTI, even 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. The default option is **Disabled.** This can cause lack of spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator.
  - **Enabled** - Enables root guard feature in the port.
  - **Disabled** - Disables root guard feature in the port.

  The root guard feature can be enabled only for the ports whose Switch Port Mode is configured as **Trunk** using **Layer2 Management > Port Manager > Port Basic Settings** screen.

- **BPDU Gaurd** - Select the administrative status for the BPDU guard feature in the port.This feature configures BPDU guard globally in MSTP and this global BPDU is applicable if and only if no port specific BPDU Guard is configured. The default option is **Disable.** The list contains:
  - Enabled - Enables BPDU Guard feature on edge ports globally and. moves the port to disabled discarding state when BPDU is received on the edge ports
  - Disabled - Disables BPDU Guard feature on edge ports globally.
- **Error Recovery** - Enter the amount of time to bring the interface out of the error-disabled (err-disabled) state. This value ranges from 30 to 65535 in 100th of seconds. The default value is 30000 = **300 seconds**.

Buttons	**Apply** - To modify attributes for the selected entry and save the changes.

20.4 MSTP VLAN Mapping

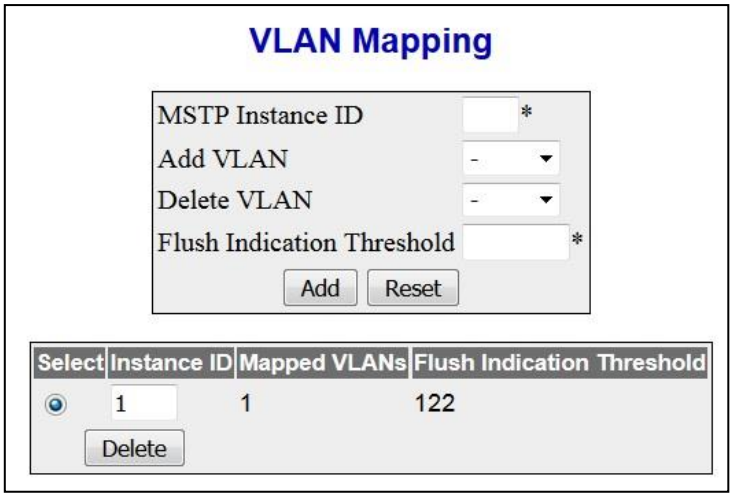


Figure 20-4 : MSTP VLAN Mapping

Screen Objective	This screen allows the user to map / unmap VLANs for each instance of MSTP and create/delete instance specific information for the member ports of the VLAN. The instance specific information for the port in one instance is independent of its information in other instance.
☞	This screen cannot be configured if the MSTP **System Control** status is set as **Shutdown** for the context selected using the **Context Selection** screen.
Navigation	**Layer2 Management** > **MSTP** > **VLAN Mapping**
Fields	• **Select** - Select the instance Id for which the mapping is to be deleted. • **MSTP Instance ID** - Enter an integer value that is used to uniquely identify an instance of the MSTP. This value ranges from 1 to 64. ✎ The mstp instance id depends on the Maximum MSTP instance configured in the Global Configuration page. ✎ Any external Agent can separately provide ESPs. The ESPs do not use spanning tree. • **Add VLAN** - Select the VLAN that should be mapped to the MSTP instance. The list contains VLAN Name of all the VLANs available in the switch. The mapping of VLAN to the MSTP instance is not done again, if the VLAN is already mapped to that instance. • **Delete VLAN** - Select the VLAN that should be unmapped from the MSTP instance. The list contains VLAN Name for the VLANs available in the switch. The unmapping of VLAN from the MSTP instance is not done, if the VLAN is already unmapped from that instance.

- **Mapped VLANs** - Displays the VLAN id mapped to the spanning tree instance specified. All the Instance Specific information for the member ports of the Vlan will be created..
- **Flush Indication Threshold** - Enter the number of flush indications to go before the flush-interval timer method triggers. This value ranges from 0 to 65535. The default value is 0

  The flush indication threshold value can be configured only when flush interval value is other than default value.

  When flush indication threshold is default value and flush interval is non-default value, instance based flushing occurs during the first flush indication trigger.

  When the flush indication threshold value is non-default(x) and flush-interval value is non-default, port & instance based flushing is triggered until the threshold(x) is reached. Once the threshold is reached, instance based flushing is triggered & timer starts..

Buttons

- **Add** - To add and save new configuration.
- **Reset** - To reset to default value for respective fields and discard all user inputs.
- **Delete** - To delete the selected entry.

20.5 MSTP Port Settings

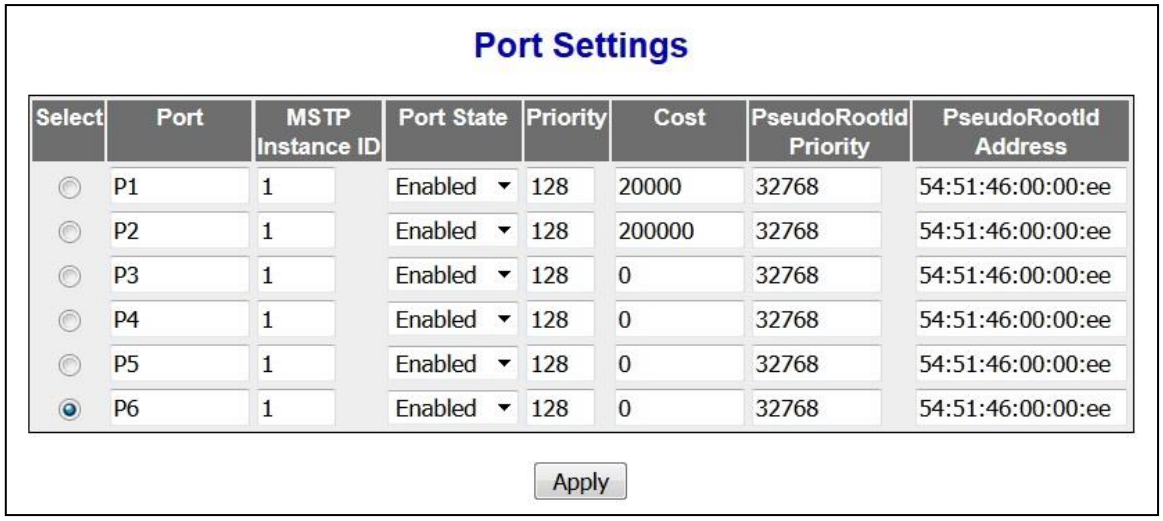


Figure 20-5 : MSTP Port Settings

Screen Objective	This screen allows the user to configure port specific information for all ports available in the switch on per port basis. It also allows the user to assign ports to specific MSTP instances so that the instances can use the port information.
☞	The parameters in the screen are not populated with the values (the screen is blank), if the MSTP **System Control** status is set as **Shutdown** for the context selected using the **Context Selection** screen. This screen can be configured only if MSTP Instance is created using the **VLAN Mapping** screen
Navigation	**Layer2 Management** > **MSTP** > **Port Settings**
Fields	• **Select** - Click to select the port for which the configuration needs to be applied. • **Port** - Displays the port number. • **MSTP Instance ID** - Displays an integer value that is used to uniquely identify an instance of the MSTP. This value ranges from 1 to 64. ✎ This field displays the Instance ID created using the **VLAN Mapping** screen • **Port State** - Select the status of the MSTP in the port. The list contains: – **Enabled** – Enables MSTP in the port. The port participates in the STP process and is ready to transmit/receive BPDUs and data. – **Disabled** – Disables MSTP in the port. The port does not participate in the STP process and is not ready to transmit/receive BPDUs and data

- **Priority** - Enter the priority value that is assigned to the port. This value is used during the role selection process. The four most significant bits of the Port Identifier of the Spanning Tree instance can be modified by setting the Cist Port Priority value.. The values that are set for Port Priority must be in steps of 16.This value ranges from 0 to 240. The default value is **128**..

- **Cost** - Enter the value that contributes to the path cost of paths towards the CIST Root which includes this port. The paths' path cost is used during calculation of shortest path to reach the MSTI root. The path cost represents the distance between the root port and designated port. This value ranges from 0 to 200000000.The default value is **200000** for all physical ports and **199999** for port channels.

  The default value is used as the path cost, if this field is not configured and the **Dynamic Path Cost Calculation** and **Speed Change Path Cost Calculation** are set as False. The dynamically calculated path cost is used if the path cost is not manually configured and one of these **Fields** is set as True.

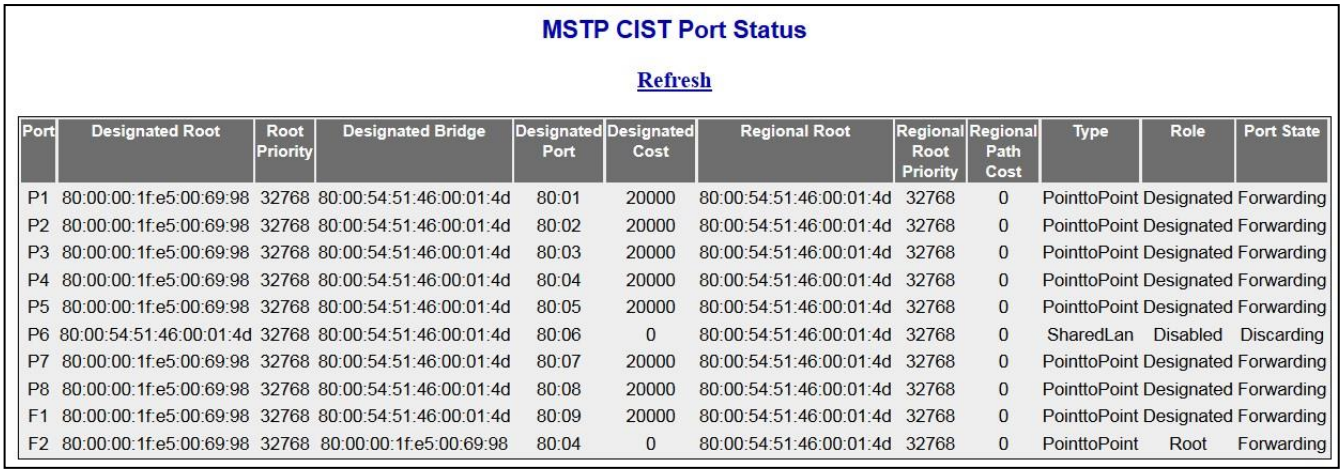
  The configured value is used as the path cost irrespective of the status (True or False) of the **Dynamic Path Cost Calculation** and **Sped Change Path Cost Calculation.**

- **PseudoRootId Priority** - Enter the priority of the pseudo root. This value is used by port configured as L2GP (the field **Layer2-Gateway Port** is set as **True**). This value ranges from 0 to 61440. The default value is **32768**. The value should be set in steps of 4096, that is, you can set the value as 0, 4096, 8192, 12288 and so on.

- **PsuedoRootId Address** - Enter the unicast MAC address of the pseudo root. This value is used by port configured as L2GP (the field **Layer2-Gateway Port** is set as **True**). The default value is 00:08:02:03:04:01.

Buttons	**Apply** - To modify attributes for the selected entry and save the changes.

20.6 MSTP CIST Port Status



MSTP CIST Port Status

Refresh

Port	Designated Root	Root Priority	Designated Bridge	Designated Port	Designated Cost	Regional Root	Regional Root Priority	Regional Path Cost	Type	Role	Port State
P1	80:00:00:1f:e5:00:69:98	32768	80:00:54:51:46:00:01:4d	80:01	20000	80:00:54:51:46:00:01:4d	32768	0	PointtoPoint	Designated	Forwarding
P2	80:00:00:1f:e5:00:69:98	32768	80:00:54:51:46:00:01:4d	80:02	20000	80:00:54:51:46:00:01:4d	32768	0	PointtoPoint	Designated	Forwarding
P3	80:00:00:1f:e5:00:69:98	32768	80:00:54:51:46:00:01:4d	80:03	20000	80:00:54:51:46:00:01:4d	32768	0	PointtoPoint	Designated	Forwarding
P4	80:00:00:1f:e5:00:69:98	32768	80:00:54:51:46:00:01:4d	80:04	20000	80:00:54:51:46:00:01:4d	32768	0	PointtoPoint	Designated	Forwarding
P5	80:00:00:1f:e5:00:69:98	32768	80:00:54:51:46:00:01:4d	80:05	20000	80:00:54:51:46:00:01:4d	32768	0	PointtoPoint	Designated	Forwarding
P6	80:00:54:51:46:00:01:4d	32768	80:00:54:51:46:00:01:4d	80:06	0	80:00:54:51:46:00:01:4d	32768	0	SharedLan	Disabled	Discarding
P7	80:00:00:1f:e5:00:69:98	32768	80:00:54:51:46:00:01:4d	80:07	20000	80:00:54:51:46:00:01:4d	32768	0	PointtoPoint	Designated	Forwarding
P8	80:00:00:1f:e5:00:69:98	32768	80:00:54:51:46:00:01:4d	80:08	20000	80:00:54:51:46:00:01:4d	32768	0	PointtoPoint	Designated	Forwarding
F1	80:00:00:1f:e5:00:69:98	32768	80:00:54:51:46:00:01:4d	80:09	20000	80:00:54:51:46:00:01:4d	32768	0	PointtoPoint	Designated	Forwarding
F2	80:00:00:1f:e5:00:69:98	32768	80:00:00:1f:e5:00:69:98	80:04	0	80:00:54:51:46:00:01:4d	32768	0	PointtoPoint	Root	Forwarding

Figure 20-6 : MSTP CIST Port Status

Screen Objective	This screen allows the user to view information maintained by every port of the switch for CIST
☞	The parameters in the screen are not populated with the values (the screen is blank), if the MSTP **System Control** status is set as **Shutdown** for the context selected using the **Context Selection** screen.
Navigation	**Layer2 Management** > **MSTP** > **CIST Port Status**
Fields	• **Port** - Displays the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number). • **Designated Root** - Displays the unique identifier of the bridge recorded as the CIST root in the transmitted configuration BPDUs. This value is an 8-byte octet string. For example, 80:00:00:01:02:03:04:05. • **Root priority** - Displays the Bridge Priority configured in **Global configuration** Screen that represents the priority of the bridge recorded as the CIST root in the configuration BPDUs transmitted. This value ranges from 0 to 61440. The default value is **32768**. • **Designated Bridge** - Displays the unique identifier of the bridge, which the port considers to be the designated bridge for the port's segment. The designated bridge is the only bridge allowed to forward frames to and from the segment. This value is an 8-byte octet string. For example, 80:00:00:01:02:03:04:05. • **Designated Port** - Displays the identifier of the port on the Designated Bridge for the port's segment. This represents the port through which the Designated Bridge forwards frames to and from the segment. This value is a 2-byte octet string. For example, 80:05.

- **Designated Cost** - Displays the Path Cost of the Designated Port of the segment connected to the port. This value ranges from 1 to 200000000.
- **Regional Root** - Displays the unique identifier of the bridge recorded as the CIST regional root in the configuration BPDUs transmitted. This value is an 8-byte octet string. For example, 80:00:00:01:02:03:04:05.
- **Regional Root Priority** - Displays the Bridge Priority that represents the priority of the bridge recorded as the CIST regional root in the configuration BPDUs transmitted. This value ranges from 0 to 61440. The default value is **32768**.
- **Regional Path Cost** - Displays the port's Path Cost that contributes to the cost of paths (including the port) towards the CIST Regional Root. This value ranges from 1 to 200000000.
- **Type** - Displays the operational Point-to-Point Status of the LAN segment attached to the port. The values can be:
  - **PointtoPoint** – Port is treated as if it is connected to a point-to-point link.
  - **SharedLan** – Port is treated as if it is having a shared media connection.

  The User can set the values directly or can set as **Auto** for the switch to decide about the point-to-point status, in the field Point-to-Point Status provided in the screen **CIST Settings**.
- **Role** - Displays the current role of the port for the spanning tree instance. The values can be:
  - **Disabled** – Specified that the port is disabled manually (**Port State**) or automatically (Link status in **Layer2 Management > Port Manager > Basic Settings**). It does not take part in the spanning tree process.
  - **Alternate** – Specifies that the port is acting as an alternate path to the root bridge. It is blocked and not used for traffic. It is enabled and declared as the root port, if the current root port is blocked.
  - **Backup** – Specifies that the port is acting as a backup path to a segment where another bridge port already connects... It is blocked and not used for traffic. It is enabled and declared as the designated port, if the active designated port is blocked.
  - **Root** – Specifies that the port is used to forward data to root bridge directly or through an upstream LAN segment.
  - **Designated** – Specifies that the port is used to send and receive packets to/from a specific downstream LAN segment/device. Only one designated port is assigned for each segment.
- **Port State** - Displays the current state of the port as defined by the common STP. The values can be:
  - **Disabled** – Specifies that the Port is disabled manually (Port State) or automatically (Link). It does not take part in the spanning tree process.
  - **Discarding** – Specifies that the port is in the Discarding state i.e. No user data is sent over the port.

- **Learning** – Specifies that the port is in the Learning state i.e. The port is not forwarding frames yet, but is populating its MAC-address-table by learning source addresses from received frames and storing them in the switching database for using these details while sending and receiving data.
- **Forwarding** – Specifies that the port is in the Forwarding state i.e. the port is operational by sending and receiving data based on the formed spanning tree topology which is loop free.

20.7 MSTP Bridge Priority

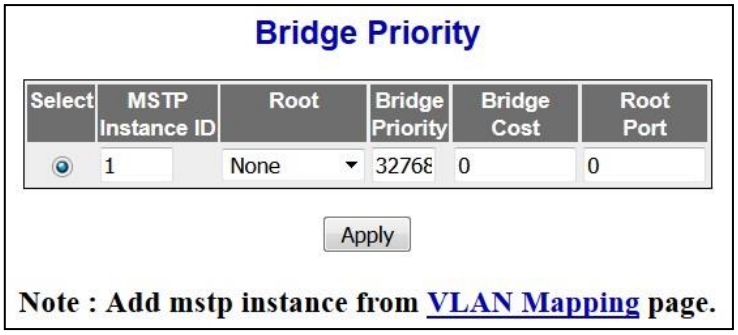


Figure 20-7 : MSTP Bridge Priority

Screen Objective	This screen allows the user to configure the bridge priority to be assigned for the specified VLAN
☞	Bridge Priority can be configured only if MSTP Instance is created using the **VLAN Mapping** screen.
Navigation	**Layer2 Management > MSTP > Bridge Priority**
Fields	• **Select**- Select the MSTP Instance ID for which the configuration needs to be applied. • **MSTP Instance ID** - Displays the integer value that uniquely identifies an instance of the MSTP.This value ranges from 1 to 64. ✎ This value is the instance ID created using the **VLAN Mapping** screen. ✎ Any external Agent can separately provide ESPs. The ESPs do not use spanning tree. • **Root** - Select the root type for the given vlan interface. The list contains; – primary - Configures the switch to become root for a given VLAN. The priority of the switch is lowered until it becomes root. – secondary - Configures the switch to become backup root for a given VLAN. The priority of the switch is lowered until it becomes one priority higher than the root, so it can become root if the current root fails. • **Bridge Priority** - Enter the priority value that is assigned to the switch. This value is used during the election of CIST root, CIST regional root and IST root.This value ranges from 0 to 61440. The Default value is **32768**. ✎ The value should be set in increments of 4096, For e.g., 0, 4096, 8192, 12288 and so on. • **Bridge Cost** - Displays the Cost of the path to the MSTI Regional Root seen by this bridge. This is a read-only field.

- **Root Port** - Displays the Port Number of the Port which offers the lowest path cost from this bridge to the CIST Root Bridge.This is a read-only field

Buttons

- **Apply** - To modify attributes for the selected entry and save the changes.

Chapter 20

RSTP

RSTP (Rapid Spanning Tree Protocol) is a portable implementation of the IEEE 802.1D standard. It provides rapid recovery of connectivity following the failure of a bridge/bridge port or a LAN. It reduces the time to reconfigure the active topology of the network when physical topology or topology configuration parameters changes. It provides increased availability of MAC service when there is a reconfiguration or failure of components in a bridged LAN. It can inter-operate with legacy STP bridges without any change in the configuration.

The RSTP provides an optional capability for:

- High availability
- Executing multiple instances of the protocol
- Provider bridging

To access RSTP screens, click **Layer2 Management > RSTP**

The RSTP related parameters are configured through the screens displayed by the following tabs:

- Global Settings
- Basic Settings
- Port Settings
- Port Status

By default, the tab **Global Settings** displays the **Global Configuration** screen.

21.1 RSTP Global Configuration

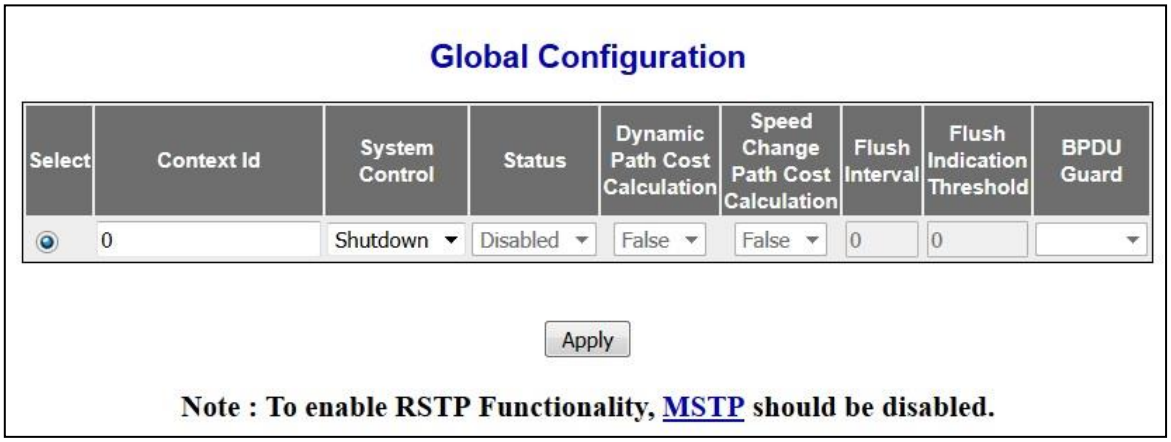


Figure 21-1 : RSTP Global Configuration

Screen Objective	This screen allows the user to configure, for each available virtual contexts, the RSTP module parameters used globally in the switch for all ports available in the switch
☞	To enable RSTP, MSTP should be disabled in the selected context.
Navigation	**Layer2 Management > RSTP > Global Settings**
Fields	• **Select** - Click to select the context for which the configuration needs to be applied. • **Context Id** - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This is a read-only field, fixed at 0. • **System Control** - Select the administrative system control status requested by management for the RSTP feature. The default option is **Shutdown**. The list contains: – Start –Specifies that all resources required by RSTP should be allocated and RSTP should be supported in the device on all ports... – Shutdown – Specifies that RSTP should be shutdown in the device on all ports and all allocated memory must be released. ✎ The administrative status can be set as Shutdown, only if the RSTP Status is set as Disabled. The status can be set as Start, only if the MSTP System Control is set as Shutdown using the **Layer2 Management > MSTP > GlobalConfiguration** screen.

- **Status** - Select the administrative module status requested by management for the RSTP module. RSTP provides rapid recovery of connectivity following the failure of a bridge/bridge port or a LAN. The default option is **Disabled**. The list contains:
  - Enabled – Enables the RSTP in the device on all the ports. Disabled – Disables the RSTP in the device on all the

    RSTP can be enabled globally in the switch, only if the RSTP System Control status is set as Start.

- **Dynamic Path Cost Calculation** - Select whether the dynamic path cost calculation is allowed . The path cost represents the distance between the root port and designated port. The path cost is based on a guideline established as part of 802.1d. According to the specification, path cost is calculated by dividing the speed with bandwidth of the segment connected to the port. The default option is **False**. The list contains:
  - True – Dynamically calculates path cost based on the speed of the ports whose **Admin State** is set as **Up** at that time. The path cost is not changed based on the operational status of the ports, once calculated.
  - False – Dynamically calculates path cost based on the link speed at the time of port creation.

    The manually assigned path cost is used irrespective of the status (**True** or **False**) of the dynamic path cost calculation.

    This field cannot be configured, if the RSTP System Control is Shutdown or Status is set as Disabled.

- **Speed Change Path Cost Calculation** - Select whether the dynamic path cost is to be calculated for ports whose speed changes dynamically. This feature is mainly used for LA ports whose speed changes due to the addition and deletion of ports from the port channel. The default option is **False**. The list contains:
  - True – Specifies that path cost is dynamically calculated for ports based on their speed at that time. The path cost is calculated, if the speed of the port changes.
  - False – Specifies that path cost is not dynamically calculated for the ports based on their speed at that time.

    This field can be configured only if System Control is set as Start.

    The manually assigned path cost is used irrespective of the status (**True** or **False**) of the dynamic path cost calculation.

- **Flush Interval** - Enter the value that controls the number of flush indications invoked from spanning-tree module per instance basis. This value ranges from 0 to 500 centi-seconds. The default value is **0**.

  This field can be configured only if System Control is set as Start.

  If the flush interval timer is set to zero, port based flushing occurs(default functionality).

  If it is set to non-zero, global / port based flushing occurs and is dependent on the flush-indication-threshold value.

- **Flush Indication Threshold** - Enter the number of flush indications before the flush-interval timer method triggers. This value ranges from 0 to 65535. The default value is **0**.

  This field can be configured only if System Control is set as Start.

  When flush indication threshold is default value and flush interval is non-default value, instance based flushing occurs during the first flush indication trigger.

  When the flush indication threshold value is non-default(x) and flush-interval value is non-default, port & instance based flushing is triggered until the threshold(x) is reached. Once the threshold is reached, instance based flushing is triggered & timer starts.

- **BPDU Guard** - Select the administrative status for the BPDU guard feature in the port.This feature configures BPDU guard globally in MSTP and this global BPDU is applicable if and only if no port specific BPDU Guard is configured. The default option is **Disable.** The list contains:
  - Enable - Enables BPDU Guard feature on edge ports globally and. moves the port to disabled discarding state when BPDU is received on the edge ports
  - Disable - Disables BPDU Guard feature on edge ports globally.

Buttons

- **Apply** - To modify attributes for the selected entry and save the changes.

21.2 RSTP Basic Settings

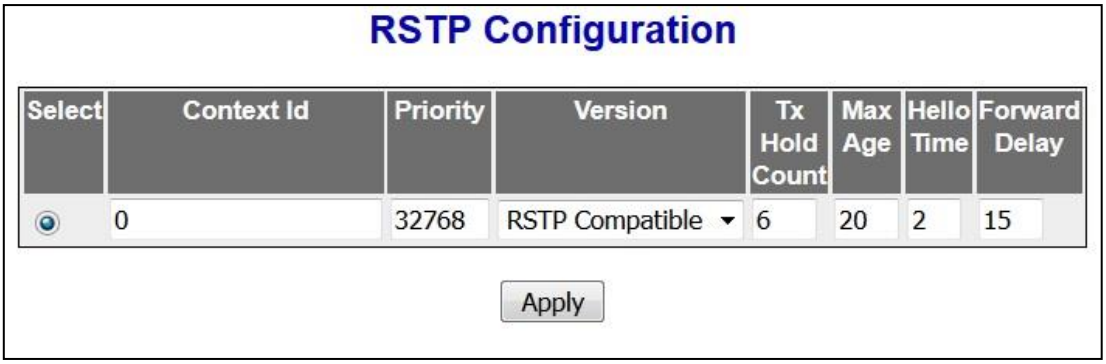


Figure 21-2 : RSTP Basic Settings

Screen Objective	This screen allows the user to configure the timers used in RSTP protocol for controlling the transmission of BPDUs during the computation of loop free topology. This configuration is applied globally in the switch on all ports
☞	This screen displays the configuration details only for the context for which the RSTP **System Control** status is set as **Start**
Navigation	**Layer2 Management > RSTP > Basic Settings**
Fields	• **Select** - Click to select the context for which the configuration needs to be applied. • **Context Id** - Displays the virtual context ID that uniquely represents a virtual switch created in the physical switch. This is a read-only field, fixed at 0. • **Priority** - Enter the priority value that is assigned to the switch. In RSTP, this value is used during the election of root. This value ranges from 0 to 61440. The default value is **32768**..The values set for Priority must be in steps of 4096. For eg, 4096, 8192, 12288 etc. • **Version** - Select the mode of STP in which the port is currentlyoperating.. The compatibility version allows the switch to temporarily operate (that is, till this configuration is reset manually) in other STP version even though the spanning tree Mode is set as some other version. This configuration is useful during cases where spanning tree Mode itself is not required to be changed. The default option is **RSTP Compatible**. The list contains: – STP Compatible – Specifies that the mode is set as STP compatible. i.e. it transmits Config/TCN BPDUs. – RSTP Compatible – Specifies that the mode is set as RSTP compatible. i.e. it transmits RST BPDUs. • **Tx Hold Count** - Enter the transmit hold count which is the number of RST BPDUs that can be transmitted in a given interval. This value is configured to avoid flooding. Port transmit state machine uses this value to

limit the maximum transmission rate. This value ranges from 1 to 10. The default value is **6**.

- **Max Age** - Enter the maximum expected arrival time (in seconds) of hello BPDUs. STP information learned from network on any port is discarded, once the configured arrival time expires. The spanning tree topology is re-computed after this time interval.. This value ranges from 6 to 40 seconds. The default value is **20** seconds.

  The maximum age should be lesser than or equal to 2*(Forward Delay - 1.0) and should be greater than or equal to 2*(HelloTime + 1.0)

- **Hello Time** - Enter the amount of time between the transmission of configuration bridge PDUs by this node.. This value can be either 1 or 2 seconds. The default value is **2** seconds.

- **Forward Delay** - Enter the value that all bridges use for ForwardDelay when the bridge is acting as the root. This value is the number of seconds, a port waits before changing from the blocking state to the forwarding state.. This value ranges from 4 to 30 seconds. The default value is **15** seconds.

Buttons	**Apply** - To modify attributes for the selected entry and save the changes.

21.3 RSTP Port Settings

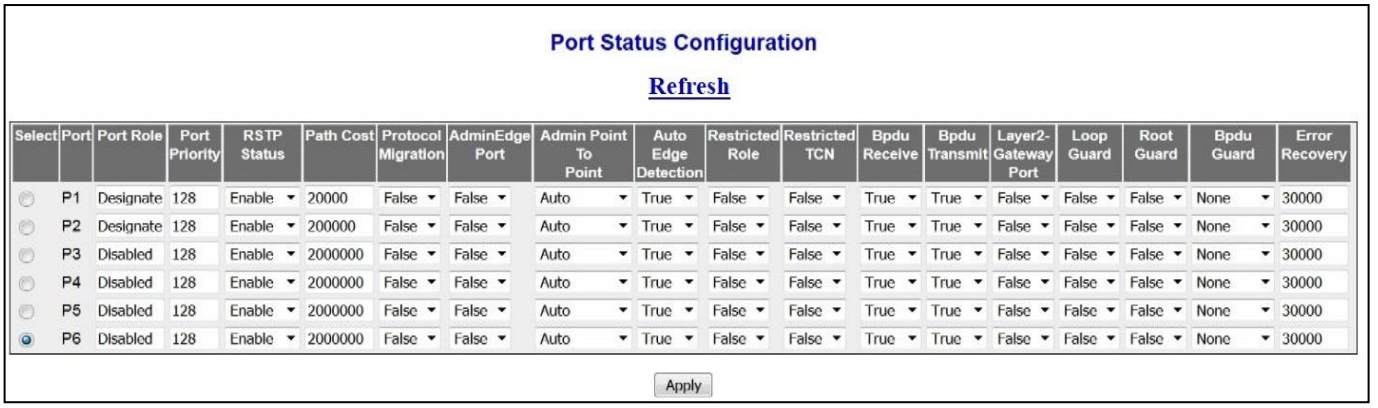


Figure 21-3 : RSTP Port Settings

Screen Objective	This screen allows the user to configure the port information for RSTP used during computation of loop-free topology
☞	The parameters in the screen are not populated with the values (the screen is blank), if the RSTP **System Control** status is set as Shutdown for the context selected using the **Context Selection** screen.
Navigation	**Layer2 Management > RSTP > Port Status Configuration**
Fields	• **Select** - Click to select the port for which the configuration needs to be applied. • **Port** - Displays the port number. ✎ Only the ports whose Admin State are set as **Up**, are displayed. • **Port Role** - Displays the current role of the port for the spanning tree. The values can be: – **Disabled** – Specifies that the port is disabled manually (**RSTP Status**) or automatically (**Link**). It does not take part in the spanning tree process. – **Alternate** – Specifies that the port is acting as an alternate path to the root bridge. It is blocked and not used for traffic. It is enabled and declared as the root port, if the root port is blocked. – **Backup** – Specifies that the port is acting as a backup path to a segment where another bridge port already connects. The port is blocked and not used for traffic, and is enabled and declared as the designated port, if the active designated port is blocked. – **Root** – Specifies that the port is used to forward data to root bridge directly or through an upstream LAN segment. – **Designated** – Specifies that the port is used to send and receive packets to/from a specific downstream LAN segment/device. Only one designated port is assigned for each segment.

- **Port Priority** - Enter the priority value that is assigned to the port. This value is used during the **Port Role** Selection process. This value ranges from 0 to 240. The default value is **128**. This value should be set in steps of 16, eg 0, 16, 32, 48 and so on.

- **RSTP Status** - Select the administrative module status requested by management for the RSTP Module on the port. This enables or disables.RSTP status of the port. The default option is **Enable**. The list contains:
  - **Enable** – Enables RSTP in the device on the port. The port participates in the STP process and is ready to transmit/receive BPDUs and data.
  - **Disable** – Disables RSTP in the device on the port. The port does not participate in the STP process and is not ready to transmit/receive BPDUs and data.

- **Path Cost** - Enter the path cost that contributes to the path cost of paths containing the port. The paths' path cost is used during calculation of shortest path to reach the root. The path cost represents the distance between the root port and designated port. This value ranges from 0 to 200000000. The default value is **200000** for all physical ports and **199999** for port channels.

  The default value is used as the path cost, if this field is not configured and the **Dynamic Path Cost Calculation** and **Speed Change Path Cost Calculation** are set as False. The dynamically calculated path cost is used if the path cost is not manually configured and one of these **Fields** is set as True.

  The configured value is used as the path cost irrespective of the status (True or False) of the **Dynamic Path Cost Calculation** and **Sped Change Path Cost Calculation.**

  The path cost value is calculated automatically based on the port speed maintained by CFA module, if the value is set as 0.

- **Protocol Migration** - Select the protocol migration state of the port.This is used to control the protocol migration mechanism that enables the module to interoperate with legacy 802.1D switches. The default option is **False**. The list contains:
  - **True** – Specifies that the port transmits BPDUs based on the spanning tree protocol supported by the receiving switch. The port is forced to transmit RSTP BPDUs.
  - **False** – Specifies that port does not perform protocol migration mechanism. The port always transmits the standard RSTP BPDUs.

  This field cannot be configured, if the RSTP Status is set as Disable.

  The protocol migration triggers the transmission of RSTP BPDUs only once, when set as True. The protocol migration changes automatically as False, once the RSTP BPDU is transmitted.

- **Admin Edge Port** - Select the administrative status of the Edge Port parameter. The default option is **False**. The list contains:

- **True** – Sets the port as an edge port the **Port State** is immediately set as **forwarding**). It is connected directly to a single end station. It allows RSTP to converge faster and does not wait to receive BPDUs.
- **False** – Sets the port as a non-Edge port the spanning tree process is performed using the RSTP). It is connected to a routing device such as switch.

. The value of the Edge Port parameter is automatically updated, if the **Auto Edge Detection** is set as **True**.

- **Admin Point-to-Point** - Select the administrative point-to-point status of the LAN segment attached to the port. The default option is **Auto**. The list contains:
  - **ForceTrue** – Specifies that port is connected to a point-to-point link.
  - **ForceFalse** – Specifies that port is having a shared media connection.
  - **Auto** – Specifies that the ports as having a shared media connection or a point-point link based on the prevailing conditions.

Port is considered to have a point-to-point link if,

- It is an aggregator and all of its members can be aggregated.
- The MAC entity is configured for full **Duplex** operation, either manually or through auto negotiation process (negotiation **Mode** is set as **Auto**).

- **Auto Edge Detection** - Select whether the Edge Port parameter of the port is detected automatically or configured manually. The default option is **True**. The list contains:
  - **True** – Specifies that detection of port as Edge Port happens automatically. The port is set as edge port, if no BPDU is received on the port. The port is set as non-edge port, if any BPDU is received by that port. This overrides the value set in the field **Admin Edge Port**, based on the reception of BPDU.
  - **False** – Specifies that automatic detection of edge port is disabled. This uses the manually configured value for the Edge Port parameter.

- **Restricted Role** - Select whether the selection of port **Role** as root can be blocked during the role selection process. This feature allows the user to block switches external to a core region of the network from influencing the spanning tree active topology. The default option is **False**. The list contains:
  - True – Blocks the port from being selected as root port for the topology, even if it has the best spanning tree priority vector. It is selected as an alternate port after the root port is selected.

The blocking of port from being selected as a root port may cause lack of spanning tree connectivity.

  - False – Includes all available ports of the topology, in the root selection process to select the root.

- **Restricted TCN** - Select the status of transmission of the received topology change notifications and topology changes to the other ports in the network. This feature allows the user to block switches external to a core

region of the network from causing address flushing in the region. The default option is **False**. The list contains:

- **True** – Blocks the port from propagating the received topology change notifications and topology changes to other ports.

  The blocking of port may cause temporary loss of connectivity after changes in a spanning tree active topology as a result of persistent incorrectly learnt station location information.

- **False** – Allows the port to propagate the received topology change notifications and topology changes to other ports.

- **Bpdu Receive** - Select the processing status of the received RSTP BPDUs. The default option is **True**. The list contains:
  - **True** – Allows normal processing of the RSTP BPDUs received on the port.
  - **False** – Discards the RSTP BPDUs received on the port.

- **Bpdu Transmit** - Select the BPDU transmission status of the port. The default option is **True**. The list contains:
  - **True** – Transmits the RSTP BPDUs from the port.
  - **False** – Blocks the transmission of RSTP BPDUs from the port.

  This field should be set as False, for ports to be configured a Layer-2 Gateway Port.

- **Layer2-Gateway Port** - Select whether the port functions as a normal port or layer2 gateway port.. The default option is **false**. The list contains:
  - **True** – Specifies that the port operates as a Layer2 Gateway Port.
  - **False** – Specifies that the port operates as a normal Port.

  BPDU Transmit , Restricted Role and **Restricted TCN** should be set as False, before configuring the port as a Layer2 gateway port.

  L2GP operates similar to that of the normal port operation but pretends to continuously receive BPDUs when **Admin State** is set as **Up**

- **Loop Guard** - Select the status of loop guard.The Loop Guard feature does age out the information even if the peer does not send information. If the port continues to receive information through BPDUs, the operation on this port will be normal.. This is useful when the neighbor bridge is faulty, that is, the bridge cannot send BPDUs but continues to send data traffic. The default option is **False**. The list contains:
  - **True** – Enables the loop guard in the port.
  - **False** – Disables the loop guard in the port

- **Root Gaurd** - Select the administrative status for the root guard feature in the port. This feature when enabled causes the Port not to be selected as Root Port for the CIST or any MSTI, even 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. The default option is **Disabled.** This can cause lack of spanning tree connectivity. It is set by a network administrator

to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator.

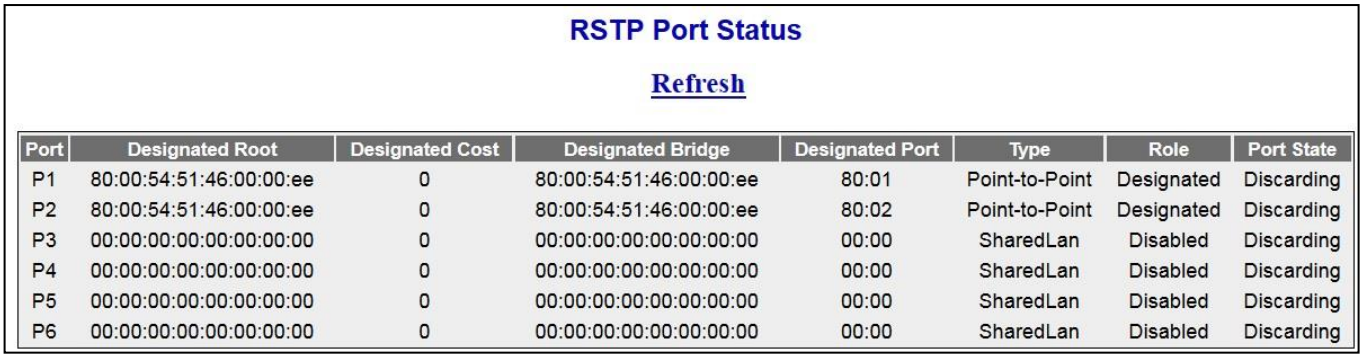
- **Enabled** - Enables root guard feature in the port.
- **Disabled** - Disables root guard feature in the port.

> The root guard feature can be enabled only for the ports whose Switch Port Mode is configured as **Trunk** using **Layer2 Management > Port Manager > Port Basic Settings** screen.

- **BPDU Gaurd** - Select the administrative status for the BPDU guard feature in the port.This feature configures BPDU guard globally in MSTP and this global BPDU is applicable if and only if no port specific BPDU Guard is configured. The default option is **Disable.** The list contains:
  - **Enabled** - Enables BPDU Guard feature on edge ports globally and. moves the port to disabled discarding state when BPDU is received on the edge ports
  - **Disabled** - Disables BPDU Guard feature on edge ports globally.
- **Error Recovery** - Enter the amount of time to bring the interface out of the error-disabled (err-disabled) state. This value ranges from 30 to 65535 in 100th of seconds. The default value is 30000 = **300 seconds**.

Buttons	**Apply** - To modify attributes for the selected entry and save the changes.

21.4 RSTP Port Status



RSTP Port Status

Refresh

Port	Designated Root	Designated Cost	Designated Bridge	Designated Port	Type	Role	Port State
P1	80:00:54:51:46:00:00:ee	0	80:00:54:51:46:00:00:ee	80:01	Point-to-Point	Designated	Discarding
P2	80:00:54:51:46:00:00:ee	0	80:00:54:51:46:00:00:ee	80:02	Point-to-Point	Designated	Discarding
P3	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
P4	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
P5	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding
P6	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Discarding

Figure 21-4 : RSTP Port Status

Screen Objective

This screen allows the user to view information maintained by every port of the switch for RSTP

The parameters in the screen are not populated with the values (the screen is blank), if the RSTP **System Control** status is set as **Shutdown** for the context selected using the **Context Selection** screen.

Navigation

Layer2 Management > RSTP > Port Status

Fields

- **Port** - Displays the port number.
- **Designated Root** - Displays the unique Identifier of the bridge recorded as the root for the segment to which the port is attached. This value is an 8-byte octet string. For example, 80:00:00:01:02:03:04:05.
- **Designated Cost** - Displays the **Path Cost** of the **Designated Port** of the segment connected to the port. This value ranges from 1 to 200000000.
- **Designated Bridge** - Displays the unique identifier of the bridge, which the port considers to be the designated bridge for the port's segment. The designated bridge is the only bridge allowed to forward frames to and from the segment. This value is an 8-byte octet string. For example, 80:00:00:01:02:03:04:05.
- **Designated Port** - Displays the identifier of the port on the Designated Bridge for the port's segment. This represents the port through which the Designated Bridge forwards frames to and from the segment. This value is a 2-byte octet string. For example, 80:05.
- **Type** - Displays the operational Admin Point to Point of the LAN segment attached to the port. The values can be:
  - **Point-to-Point** – Specifies that the port is treated as if it is connected to a point-to-point link.
  - **SharedLan** – Specifies that the port is treated as if it is having a shared media connection.

The values can be set directly or as **Auto** for the switch to decide about the point-to-point status, in the field Admin Point to Point provided in the screen **Port Status Configuration**

- **Role** - Displays the current role of the port for the spanning tree instance. The values can be:
  - **Disabled** – Specifies that the port is disabled manually (**RSTP Status** screen) or automatically (Link status in **Layer2 Management > Port Manager > Basic Settings**). It does not take part in the spanning tree process.
  - **Alternate** – Specifies that the port is acting as an alternate path to the root bridge. It is blocked and not used for traffic. It is enabled and declared as the root port, if the root port is blocked.
  - **Backup** – Specifies that the port is acting as a backup path to a segment where another bridge port already connects. It is blocked and not used for traffic. It is enabled and declared as the designated port, if the active designated port is blocked.
  - **Root** – Specifies that the port is used to forward data to root bridge directly or through an upstream LAN segment.
  - **Designated** – Specifies that the port is used to send and receive packets to/from a specific downstream LAN segment/device. Only one designated port is assigned for each segment.
- **Port State** - Displays the current state of the port as defined by the STP. The values can be:
  - **Disabled** – Specifies that the port is disabled manually (**RSTP Status**) or automatically ((Link status in **Layer2 Management > Port Manager > Basic Settings**). It does not take part in the spanning tree process.
  - **Discarding** – Specifies that the port is in the Discarding state i.e. No user data is sent over the port.
  - **Learning** – Specifies that the port is in the Learning state i.e. The port is not forwarding frames yet, but is populating its MAC-address-table by learning source addresses from received frames and storing them in the switching database for using these details while sending and receiving data.
  - **Forwarding** – Specifies that the port is in the Forwarding state i.e. the port is operational by sending and receiving data based on the formed spanning tree topology which is loop free.

Chapter 21

LLDP

LLDP (Link Layer Discovery Protocol) is a vendor-neutral Data Link Layer (neighbour discovery) protocol used by network devices for advertising their identity, capabilities, and interconnections on an IEEE 802 LAN network. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery specified in standards document 802.1AB.

LLDP performs functions similar to several proprietary discovery protocols, from Cisco, Nortel (SONMP), and Microsoft LLTD (Link Layer Topology Discovery).

LLDP data is stored in the device as a management information database (MIB) and can be queried with the Simple Network Management Protocol (SNMP) as specified in RFC 2922. The topology of an LLDP-enabled network can be discovered by querying this database.

To access LLDP screens, click **Layer2 Management > LLDP.**

The LLDP related parameters are configured through the screens displayed by the following tabs:

- Global Settings
- Basic Settings
- Interfaces
- Neighbours
- Agent Info
- Agent Details

By default, the tab **Global Settings** displays the **LLDP Global Configurations** screen.

22.1 LLDP Global Configurations

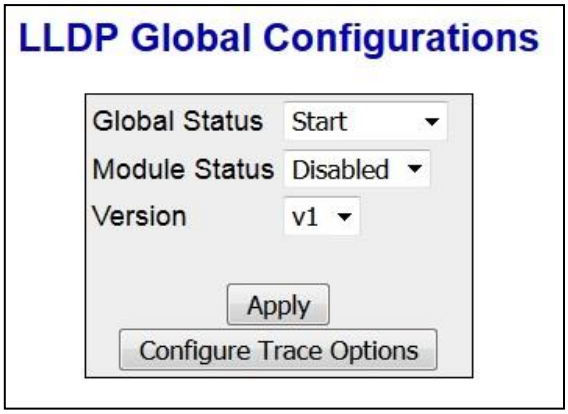


Figure 22-1 : LLDP Global Configurations

Screen Objective	This screen allows the user to enable or disable LLDP module globally and set the LLDP version number
Navigation	**Layer2 Management > LLDP > Global Settings**
Fields	• **Global Status** - Select the administrative system control status of LLDP. The options are: – **Start** - Indicates that all the resources required by LLDP module should be allocated and LLDP should be supported in the devices on all ports. – **ShutDown** - Indicates that LLDP should be shutdown in the device on all ports and all allocated memory must be released. If the Global Status is set as Shut Down, the Module Status cannot be enabled. • **Module Status** - Select the administrative module status of LLDP module. The list contains – **Enabled** - Indicates that LLDP is enabled in the device and can be enabled port-wise – **Disabled** - Indicates that LLDP is disabled in the device and also disabled on all ports. • **Version** - Select the Version of LLDP to be used on the system. The default option is **v1(Version 1)**. The list contains; – **v1** - Enables LLDP version 1 (2005) on the port. When V1 is enabled the port can be assigned with only one MAC address. – **v2** - Enables LLDP version 2 (2009) on the port. when enabled mac-address can be assigned per port i.e. the user can have multiple lldp Agents per port
Buttons	• **Apply** - To modify attributes and save the changes. • **Configure Trace Options** - To access the **Configured Traces** screen.

22.1.1 LLDP Configured Traces

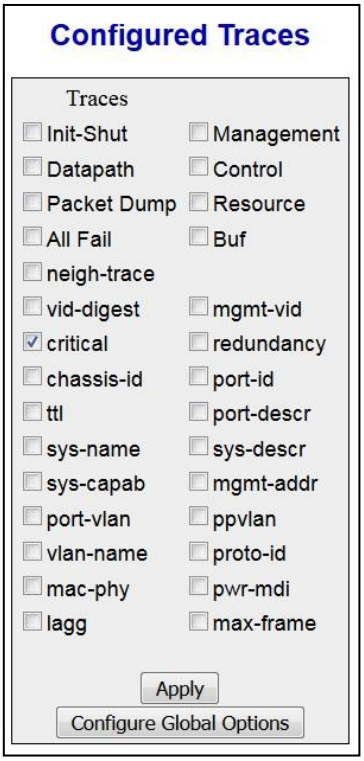


Figure 22-2 : LLDP Configured Traces

Screen Objective	This screen allows the user to enable the required debug statements useful during debug operation
Navigation	**Layer2 Management > LLDP Global Settings > LLDP Global Configuration** screen **>** click **Configure Trace Options** button
Fields	• **Traces** - Select the traces for which debug statements is to be generated. The default option is **critical.** The options are: – **Init-Shut** – Generates debug statements for init and shutdown traces. This trace is generated on failed and successful initialization and shutting down of LLDP related module and memory. – **Management** – Generates debug statements for management traces. This trace is generated when any of the LLDP features is configured. – **Datapath** – Generates the debug statements for datapath traces. This trace is generated during failure in packet processing. – **Control** – Generates debug statements for Control functionality traces. This trace is generated during failure in modification or retrieving of LLDP entries – **Packet Dump** – Generates debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets.

- **Resource –** Generates debug statements for Traces with respect to allocation and freeing of all resource expect the buffers.
- **All Fail –** Generates debug statements for all failure traces of the above mentioned traces.
- **Buffer –** Generates debug statements for traces with respect to allocation and freeing of Buffer.
- **Neigh-trace** - Generates debug statements for neighbour traces.
- **vid-digest** - Generates debug statements for vlan identifier (vid) digest type, length, and value (TLV) traces
- **mgmt-vid** - Generates debug statements for management vid tlv traces.
- **critical** - Generates debug statements for critical state machine (SEM).
- **redundancy** - Generates the debug statements for the LLDP redundancy module.
- **chassis-id** - Generates debug statements for chassis-id TLV traces.
- **port-id** - Generates debug statements for port-id TLV trace
- **ttl** - Generates debug statements for *Time To Live* (TTL) TLV trace.
- **port-descr** - Generates debug statements for the port description TLV traces.
- **sys-name** - Generates debug statements for the system name TLV traces.
- **sys-descr** - Generates debug statements for system description TLV traces.
- **sys-capab** - Generates debug statements for system capabilities TLV traces.
- **mgmt-addr** - Generates debug statements for management address TLV traces.
- **port-vlan** - Generates debug statements for port-vlan TLV traces.
- **ppvlan** - Generates debug statements for port-protocol-vlan TLV traces.
- **vlan-name** - Generates debug statements for vlan-name TLV traces.
- **proto-id** - Generates debug statements for protocol-id TLV traces.
- **mac-phy** - Generates debug statements for MAC or physical (PHY) TLV traces.
- **pwr-mdi** - Generates debug statements for power-through- (*Media Dependent Interface)* MDI TLV traces.
- **lagg** - Generates debug statements for link aggregation TLV traces.
- **max-frame** - Generates debug statements for maximum frame size TLV traces.

Buttons

- **Apply** - To modify attributes and save the changes.
- **Configure Global Options –** To access the **LLDP Global Configuration** screen

22.2 LLDP Basic Settings

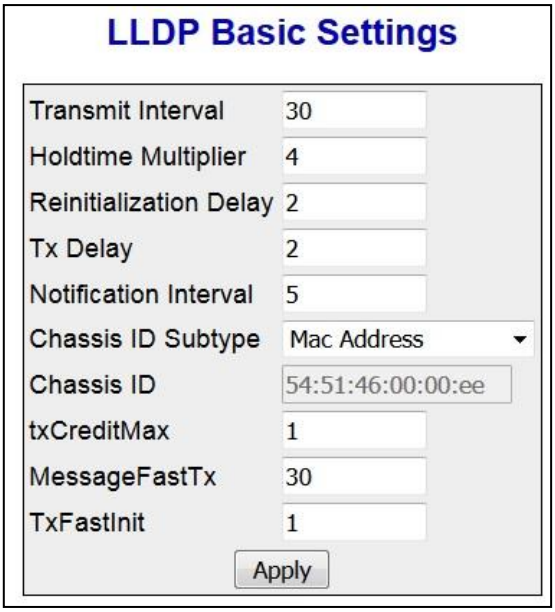


Figure 22-3 : LLDP Basic Settings

Screen Objective	This screen allows the user to configure the LLDP basic parameters
Navigation	**Layer2 Management > LLDP > Basic Settings**
Fields	• **Transmit Interval** - Enter the time interval at which the LLDP frames are transmitted on behalf of this LLDP Agent. The value should be restored from non-volatile storage after a re-initialization of the management system. The value ranges from 5 to 32768. The default value is **30** seconds. • **Holdtime Multiplier** - Enter the holdtime-multiplier value, which is the amount of time, the server should hold the LLDP. This value ranges from 2 to 10. The default value is **4**. The actual time-to-live value used in LLDP frames, transmitted on behalf of this LLDP Agent, can be expressed by the following formula: TTL = min (65535, Transmit Interval * Holdtime Multiplier). For example. If the value of Transmit Interval is 30 and value of Holdtime Multiplier is 4 then value '120' is encoded in TTL field of LLDP header. The value of this object must be restored from non-volatile storage after a re-initialization of the management system. • **Reinitialization Delay** - Enter the delay from when the port admin status becomes 'disabled' until re-initialization will be attempted. The value of this object must be restored from non-volatile storage after a re-initialization of the management system. This value ranges from 1 to 10. The default value is **2** seconds.

- **Tx Delay** - Enter the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems objects. This value ranges from 1 to 8192. The value should be lesser than or equal to (0.25 * Transmit Interval) The default value is **2** seconds.

- **Notification Interval** - Enter the time interval in which the local system generates a notification-event In the specific interval, generating more than one notification-event is not possible . If additional changes in lldpRemoteSystemsData object groups occur within the indicated throttling period, then these trap- events must be suppressed by the Agent. The value of this object must be restored from non-volatile storage after a re-initialization of the management system. This value ranges from 5 to 3600. The default value is **5**.

- **Chassis ID Subtype** - Select the source of a chassis identifier. The default option is **Mac Address**. The options are:
  - **Chassis Component** - Represents a chassis identifier based on the value of entPhysicalAlias object for a chassis component
  - **Interface Alias** - Represents a chassis identifier based on the value of ifAlias for an interface on the containing chassis.
  - **Port Component** - Represents a chassis identifier based on the value of entPhysicalAlias object for a port or backplane within the chassis.
  - **Mac Address** - Represents a chassis identifier based on the value of a unicast source address, of a port on the containing chassis.
  - **Network Address** - Represents a chassis identifier based on a network address, associated with a particular chassis. The encoded address is actually composed of two Fields. The first field is a single octet, representing the IANA AddressFamilyNumbers value for the specific address type, and the second field is the network address value.
  - **Interface Name** - Represents a chassis identifier based on the value of ifName object for an interface on the containing chassis.
  - **Local** - Represents a chassis identifier based on a locally defined value.

- **Chassis ID** - Enter the chassis identifier string.

  This field is enabled only if the Chassis ID subtype is selected as anyone of the following;

  Chassis Component - The octet string identifies a particular instance of the entPhysicalAlias object for a chassis component

  Port Component – The octet string identifies a particular instance of the entPhysicalAlias object for a port or backplane component within the containing chassis.

  Local – The Octet string identifies a locally assigned chassis ID.

- **txCreditMax** - Enter the maximum number of consecutive LLDPDUs that can be transmitted any time by the port. This value ranges from 1 to 10. The default value is **1** for LLDP Version v1 and **5** for LLDP Version v2

- **MessageFastTx** - Enter the interval at which LLDP frames are transmitted on behalf of LLDP Agent during fast transmission period. This value ranges from 1 to 3600 seconds. The default value is **30** for LLDP Version v1 and **1** for LLDP Version v2

- **TxFastInit** - This command configures the value used to initialize the txFast variable which determines the number of transmissions that are made in fast transmission mode. This value ranges from 1 to 8. The default value is **1** for LLDP Version v1 and **4** for LLDP Version v2

Buttons	**Apply** - To modify attributes and save the changes.

22.3 LLDP Interfaces Settings

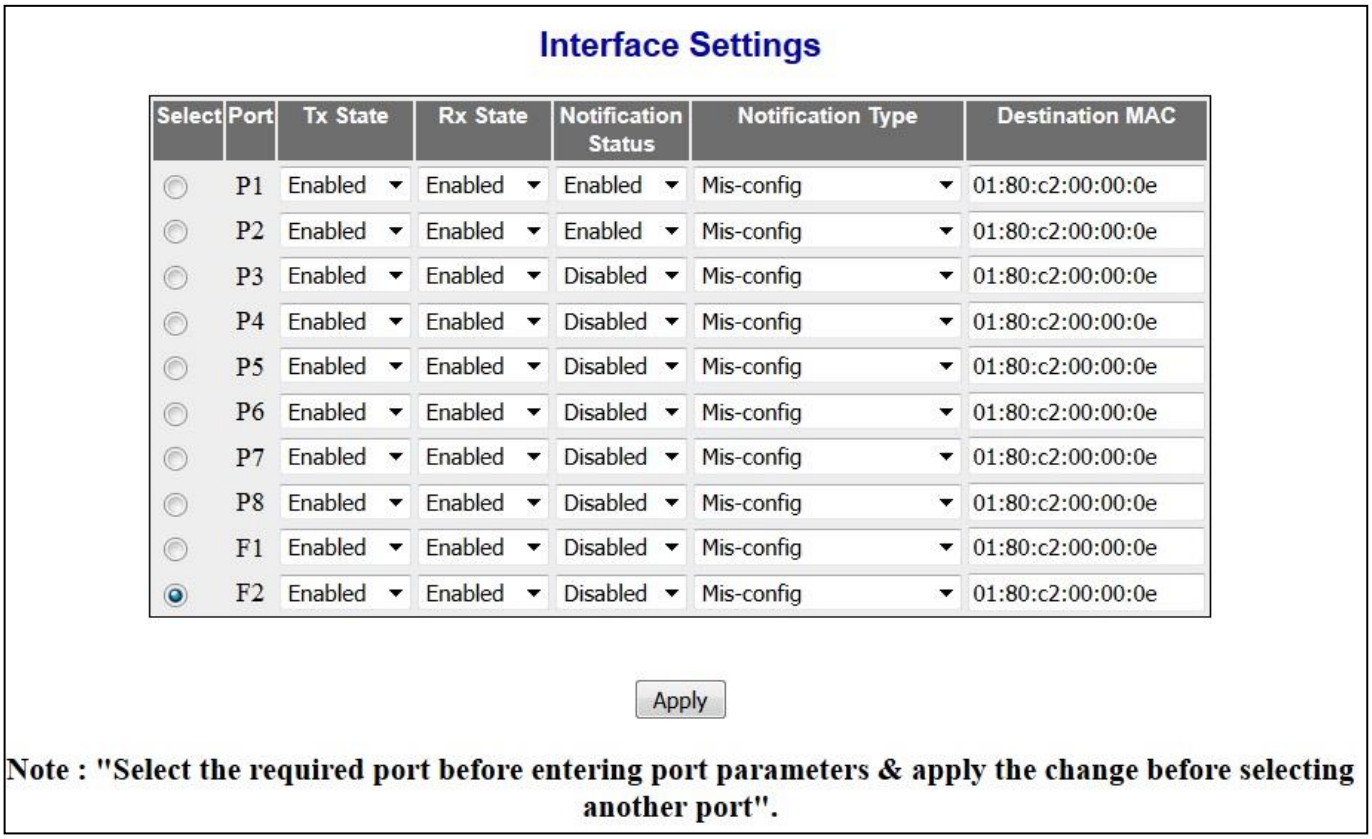


Figure 22-4 : LLDP Interface Settings

Screen Objective	This screen allows the user to configure each port of the LLDP
☞	The parameters in the screen are not populated with the values (the screen is blank), if the LLDP Global Sates is set as **Shutdown**

Navigation	**Layer2 Management > LLDP >Interface**
Fields	• **Select** - Click to select the port for which the LLDP parameters need to be configured. • **Port** - Displays the port number. • **Tx State** - Select the status of the LLDP PDU transmitter. The default option is **Enabled**. The options are: – **Enabled** - Enables transmission of LLDPDU from one of the ports of the server to the LLDP module – **Disabled** – Disables transmission of LLDPDU from one of the ports of the server to the LLDP module. • **Rx State** - Select the status of the LLDP PDU receiver. The default option is **Enabled**. The options are: – **Enabled** - Enables reception of LLDPDU from one of the ports of the server to the LLDP module – **Disabled** – Enables reception of LLDPDU from one of the ports of the server to the LLDP module • **Notification Status** - Select the notification status to be set. The default option is **Disabled**. The options are: – **Enabled** – Enables the notification status. – **Disabled** - Disables the notification status. • **Notification Type** - Select the notification type. The default option is **Mis-config**. The options are: – **Remote-Table-Change** - LLDP Agent sends trap notification to NMS whenever remote table change occurs. – **Mis-Config** - LLDP Agent sends trap notification to NMS whenever mis-configuration is identified. – **Both** - LLDP Agent sends trap notification to NMS whenever remote table change occurs or/and whenever mis-configuration is identified. • **Destination MAC** - Displays the destination mac-address to be used by the LLDP Agent for transmission on this port.
Buttons	**Apply** - To modify attributes and save the changes.

22.4 LLDP Neighbour Information

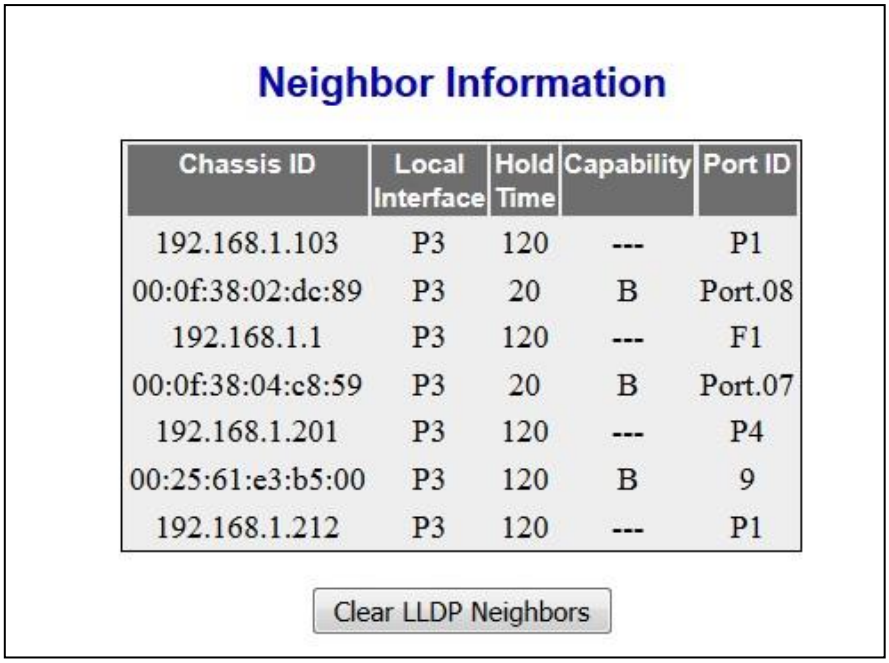


Figure 22-5 : LLDP Neighbor Information

Screen Objective	This screen allows the user to obtain the information of the adjacent server connected with the LLDP
Navigation	**Layer2 Management > LLDP >Neighbors**
Fields	**Chassis ID** - Displays the Chassis ID of the peer. This value is a string value with a maximum size of 255. Typical Values are: – **Chassis Component** - Represents a chassis identifier based on the value of entPhysicalAlias object for a chassis component – **Interface Alias** - Represents a chassis identifier based on the value of ifAlias for an interface on the containing chassis. – **Port Component** - Represents a chassis identifier based on the value of entPhysicalAlias object for a port or backplane within the chassis. – **Mac Address** - Represents a chassis identifier based on the value of a unicast source address, of a port on the containing chassis. – **Network Address** - Represents a chassis identifier based on a network address, associated with a particular chassis. The encoded address is actually composed of two Fields. The first field is a single octet, representing the IANA AddressFamilyNumbers value for the specific address type, and the second field is the network address value. – **Interface Name** - Represents a chassis identifier based on the value of ifName object for an interface on the containing chassis. – **Local** - Represents a chassis identifier based on a locally defined value.

	• **Local Interface** - Displays the local port on which the peer information is learnt.This value is a string of maximum size 255 • **Hold Time** - Displays the Hold Time advertized by the peer • **Capability** - Displays the capabilities advertized by the peer • **Port ID** - Displays the Port ID advertized by the peer
Buttons	• **Clear LLDP Neighbors** - To clear the Neighbor information

22.5 LLDP Agent Info

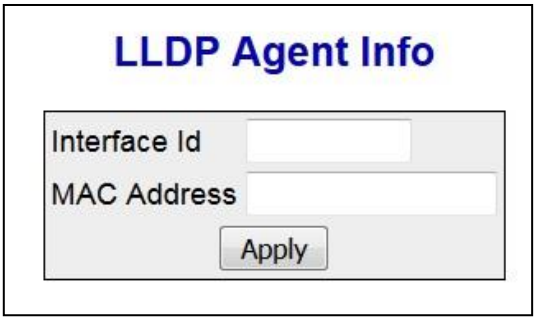


Figure 22-6 : LLDP Agent Info

Screen Objective	This screen allows the user to configure the destination mac-address to be used by the LLDP Agent for transmission on this port
Navigation	**Layer2 Management > LLDP >Agent Info**
Fields	• **Interface Id** - Enter the Interface ID for which the LLDP Agent info is to be configured. The Interface Id value ranges between 1 and 24. • **MAC Address** - Enter the MAC address to be used as LLDP Agent MAC address by the LLDP Agent on the specified port When LLDP Version is set as V1 only one MAC address can be assigned for a port. When LLDP Version is set as V2 multiple mac-address can be assigned per port i.e. the user can have multiple LLDP Agent per port
Buttons	**Apply** - To modify attributes and save the changes.

22.6 LLDP Agent Details

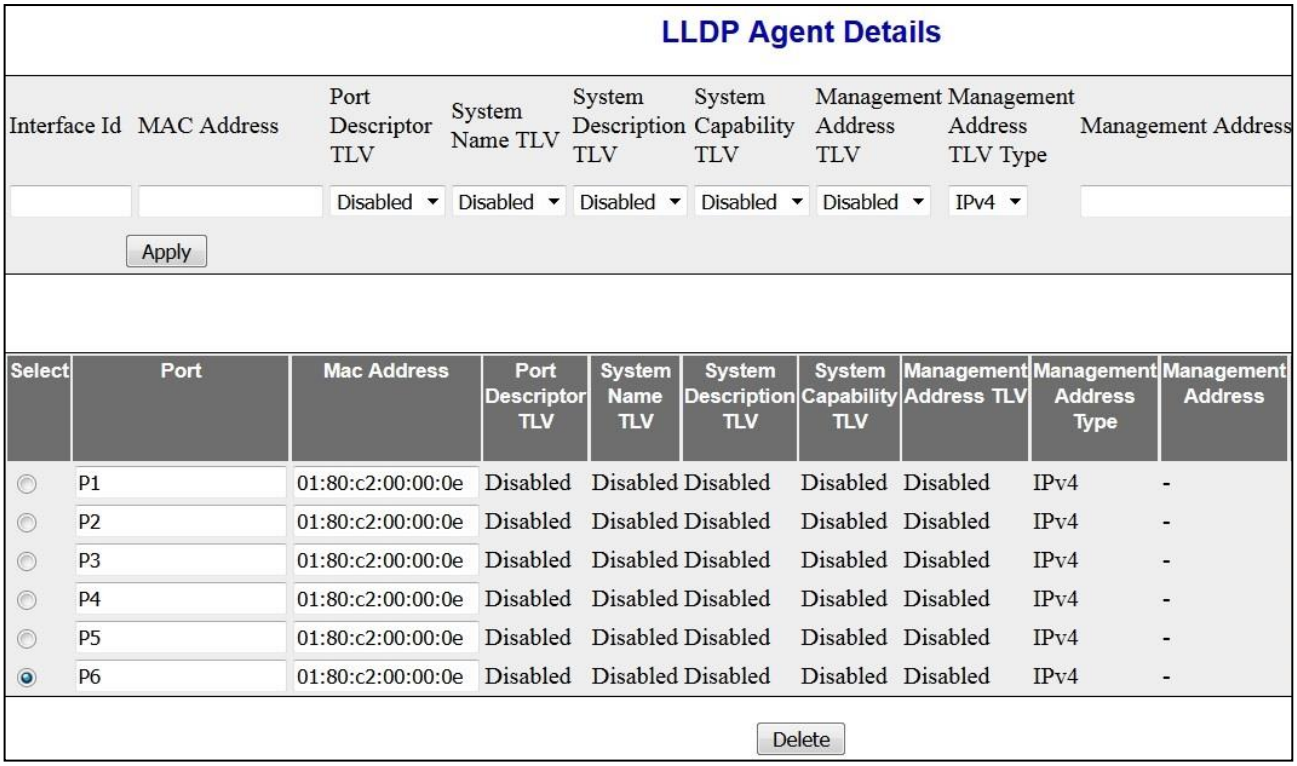


Figure 22-7 : LLDP Agent Details Part A

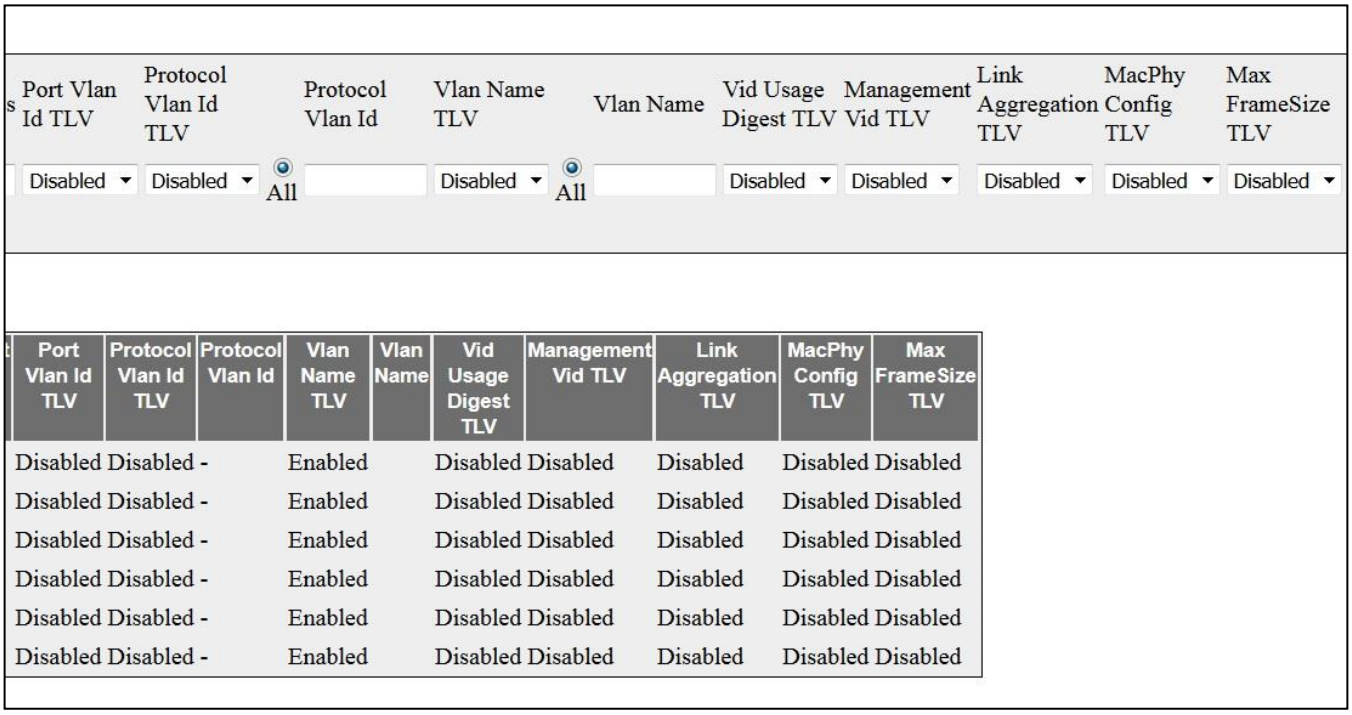


Figure 22-8 : LLDP Agent Details Part B

Screen Objective	This screen allows the user to configure the destination mac-address to be used by the LLDP Agent for transmission on this port
Navigation	**Layer2 Management > LLDP >Agent Details**
Fields	• **Interface Id** - Enter the Interface ID for which the LLDP Agent details is to be configured. This value ranges from 1 to 24. • **MAC Address** - Enter the MAC address to be used as LLDP Agent MAC address by the LLDP Agent on the specified port When LLDP Version is set as V1 only one MAC address can be assigned for a port. When LLDP Version is set as V2 multiple mac-address can be assigned per port i.e. the user can have multiple LLDP Agent per port This screen can be configured for a specific MAC address only if Agent is created with the MAC Address using the **LLDP Agent Info** screen • **Port Descriptor TLV** –Select the transmit status for Port Description TLV (Type Length Variable). The default option is **disabled**. The list contains; – **Enabled** – Indicates that LLDP Agent transmits Port Description TLV – **Disabled** - Indicates that LLDP Agent discards Port Description TLV • **System Name TLV** – Select the transmit status for System Name TLV. The default option is **disabled**. The list contains; – **Enabled** – Indicates that LLDP Agent transmits System Name TLV – **Disabled** - Indicates that LLDP Agent discards System Name TLV • **System Description TLV** – Select the transmit status for System Description TLV. The default option is **disabled**. The list contains; – **Enabled** – Indicates that LLDP Agent transmits System Description TLV – **Disabled** - Indicates that LLDP Agent discards System Description TLV • **System Capability TLV** – Select the transmit status for System Capability TLV. The default option is **disabled**. The list contains; – **Enabled** – Indicates that LLDP Agent transmits System Capability TLV – **Disabled** - Indicates that LLDP Agent discards System Capability TLV • **Management Address TLV** – Select the transmit status for Management Address TLV. The default option is **disabled**. The list contains; – **Enabled** – Indicates that LLDP Agent transmits System Capability TLV – **Disabled** - Indicates that LLDP Agent discards System Capability TLV • **Management Address TLV Type** – Select the address type for the Managment address. This list contains;

  - **All** - Selects the address type for the Management address as both IPv4 and IPv6 addresses.
  - **IPv4** - Selects the address type for the Management address as IPv4
  - **IPv6** - Selects the address type for the Management address as IPv6

- **Management Address** – Enter the Management IP address for the TLV as per the addresstype selected.

- **Port Vlan Id TLV** – Select the transmit status for Port Vlan Id TLV. The default option is **disabled**. The list contains;
  - **Enabled** – Indicates that LLDP Agent transmits Port Vlan Id TLV
  - **Disabled** - Indicates that LLDP Agent discards Port Vlan Id TLV

- **Protocol Vlan Id TLV** – Select the transmit status for Protocol Vlan Id TLV. The default option is **disabled**. The list contains;
  - **Enabled** – Indicates that LLDP Agent transmits Port Vlan Id TLV
  - **Disabled** - Indicates that LLDP Agent discards Port Vlan Id TLV

- **Protocol Vlan Id** – Enter the Protocol Vlan ID. Indicates that LLDP Agent should transmit Port Vlan Id TLV
  - **all** - Indicates that LLDP Agent transmits all Protocol Vlan Id TLV

- **Vlan Name TLV** – Select the VLAN Name TLV for enabling or disabling the transmission of the LLDP Agent. The default option is **Enabled.** The list contains;
  - **Enabled** – Indicates that LLDP Agent transmits VLAN Name TLV
  - **Disabled** - Indicates that LLDP Agent discards VLAN Name TLV

- **Vlan Name** – Enter the specific VLAN ID for which the LLDP Agent trasmits PDUs.
  - **all** - Indicates that LLDP Agent transmits through all Vlan

- **Vid Usage Digest TLV** – Select the transmit status for Vid Usage Digest TLV. The default option is **disabled**. The list contains;
  - **Enabled** – Specifies that LLDP Agent transmits Vid Usage Digest TLV
  - **Disabled** - Specifies that LLDP Agent discards Port Vid Usage Digest TLV

- **Managemet Vid TLV** – Select the transmit status for Management Vid TLV. The default option is **disabled**. The list contains;
  - **Enabled** – Specifies that LLDP Agent transmits Management Vid TLV
  - **Disabled** - Specifies that LLDP Agent discards Management Vid TLV

- **Link Aggregation TLV** – Select the transmit status for Link Aggregation TLV. The default option is **disabled**. The list contains;
  - **Enabled** – Specifies that LLDP Agent transmits Link Aggregation TLV
  - **Disabled** - Specifies that LLDP Agent discards Link Aggregation TLV

- **MacPhy Config TLV** – Select the transmit status for Link MacPhy Config TLV. The default option is **disabled**. The list contains;
  - **Enabled** – Specifies that LLDP Agent transmits MacPhy Config TLV
  - **Disabled** - Specifies that LLDP Agent discards MacPhy Config TLV
- **Max Frame Size TLV** – Select the transmit status for Max Frame Size TLV. The default optionis **disabled**. The list contains;
  - **Enabled** – Specifies that LLDP Agent transmits Max Frame Size TLV
  - **Disabled** - Specifies that LLDP Agent discards Max Frame Size TLV

Buttons	**Apply** - To modify attributes and save the changes. **Delete** - To delete the selected entry.

Chapter 22

802.1x

802.1x or PNAC provides a means of authenticating devices attached to a bridge port. It prevents access to a port when the authentication fails. 802.1X defines (802.1X) port-based authentication as a client-server based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. An authentication server validates each supplicant (client) connected to an authenticator (network access switch) port before making available any services offered by the switch or the LAN.

Until the authentication is provided, 802.1X access control allows only EAPOL (Extensible Authentication Protocol Over LAN) traffic through the port. When the authentication is provided, normal traffic is allowed through the port.

To access PNAC screens, click **Layer2 Management > 802.1X**.

The **802.1x** related parameters are configured through the screens displayed in the following tabs:

- Global Settings
- Port Settings
- Timers
- Local AS
- Radius Settings
- MacSession Info

By default, the tab **Global Settings** displays **802.1x Global Settings** screen.

23.1 802.1x Global Settings

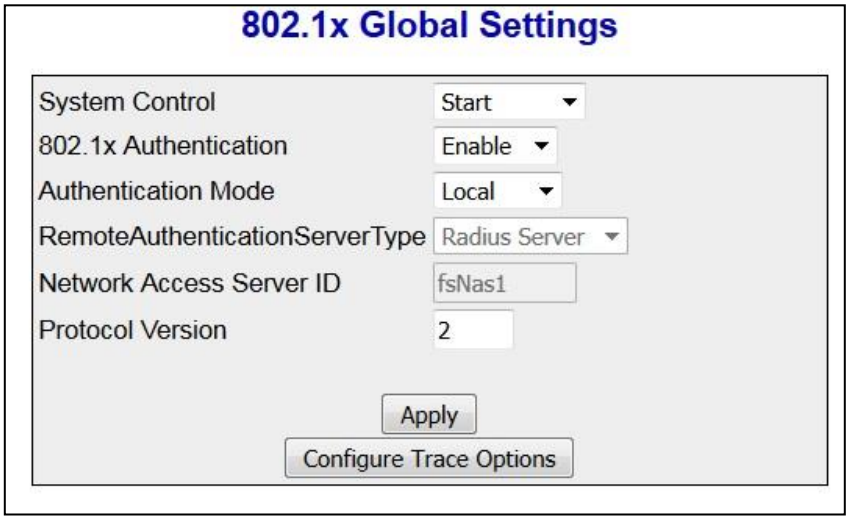


Figure 23-1 : 802.1x Global Settings

Screen Objective	This screen allows the user to configure Authentication status, Authentication mode and Authentication server type
Navigation	**Layer2 Management > 802.1x > Global Settings**
Fields	• **System Control** - Select the system control status of the PNAC module. The default option is **Start**. The options are – **Start** – Starts PNAC Module in the system. ▪ Memory Resources required by PNAC module are allocated and PNAC module starts running. ▪ Creates Memory pool, spawn the PNAC interface task. Initialize all the global data structures ▪ Create a hash table for storing the session nodes for MAC based authorization entries. ▪ Creates semaphore for controlling concurrent access to critical databases ▪ Initialize the timer submodule and PNAC Local authentication server module. – **Shutdown** – Shuts down PNAC Module ▪ All resources used by PNAC module are released to the system and the PNAC module is shut down. ▪ Initialize all the PNAC state machines. ▪ Deactivates the PNAC Local authentication server module, the timer module. Deletes the memory pool for the PNAC module and free its memory. ▪ Deletes semaphore used for database access-control.

- **802.1x Authentication** - Select the status of 802.1x based port security feature in the switch. The default option is **Enable**. The options are::
  - **Enable** – Enables 802.1x based port security feature in the switch. The switch initiates authentication and sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.
  - **Disable** – Disables 802.1x based port security feature in the switch. EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state

- **Authentication Mode** - Select the Authentication Server Location. The default option is **Local**. The options are
  - **Remote** – Radius server based authentication. It calls the AS client functions to communicate with the remote authentication server.
  - **Local** – Provides the authentication service requirements in the local database. It maintains a simple database of users who can be permitted on valid proof to access a set of Authenticator's ports. It calls the service functions of the Local AS.

- **RemoteAuthenticationServerType** - Select the Remote Authentication Server Type. The default option is **Radius Server**. The options are:
  - **Radius Server** – Sets the remote authentication server as Radius Server. RADIUS server is responsible for authentication, authorization and maintaining its account information with port-based authentication. It is a gateway that controls access to the network. RADIUS uses the User Datagram Protocol (UDP). RADIUS server acts as the centralized authentication server
  - **Tacacs Server** – Sets the remote authentication server as TACACS Server. The remote TACACS+ server is responsible for TACACS+ client communication to authenticate the user, get authorization information and send accounting information to the user. TACACS+ uses the Transmission Control Protocol (TCP). This feature is currently not supported.

  
  This field can be configured only if the Authentication Mode is set as Remote.

- **Network Access Server ID** - Enter the Network Acess Server ID, It is the server ID for which authentication is provided. The Authenticator ID originates from the Access Request packets. The value is of string type.

- **Protocol Version** - Specifies the Version Number of the Protocol. This is a read-only field.

Buttons

- **Apply** - To modify attributes and save the changes.
- **Configure Trace Options -** To access **PNAC Traces** screen

23.1.1 802.1x PNAC Traces

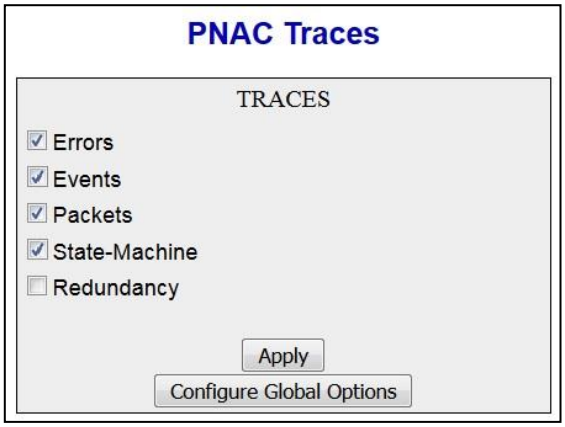


Figure 23-2 : 802.1x PNAC Traces

Screen Objective	This screen allows the user to enable the required debug statements that are useful during debug operation. A FOUR BYTE integer is used for enabling the level of tracing. Each BIT in the four byte integer represents a particular level of Trace. Combination of levels is also allowed. System errors such as memory allocation failures are notified by means of LOG messages and TRACE messages. Interface errors and protocol errors are notified by means of TRACE messages.
Navigation	**Layer2 Management > 802.1x > Global Settings > Configure Trace Options** button
Fields	• **Traces** - Select the traces for which debug statements is to be generated. The options are: – **Errors** - Generates debug statement for all failure traces of the below mentioned traces – **Events** - Generates debug statements for event handling traces. This trace is generated in case of event processing. – **Packets** - Generates debug statements for packets handling traces. This trace is generated in case of transmission or reception of packets. – **State-Machine** - Generates debug statements for state machine handling traces. This trace is generated in case of State Machine processing. – **Redundancy** - Generates debug statements for redundancy code flow traces. This trace is generated in case of redundancy processing.
Buttons	• **Apply** - To modify attributes and save the changes. • **Configure Global Options** - To access **802.1x Global Settings** screen.

23.2 802.1X Port Settings

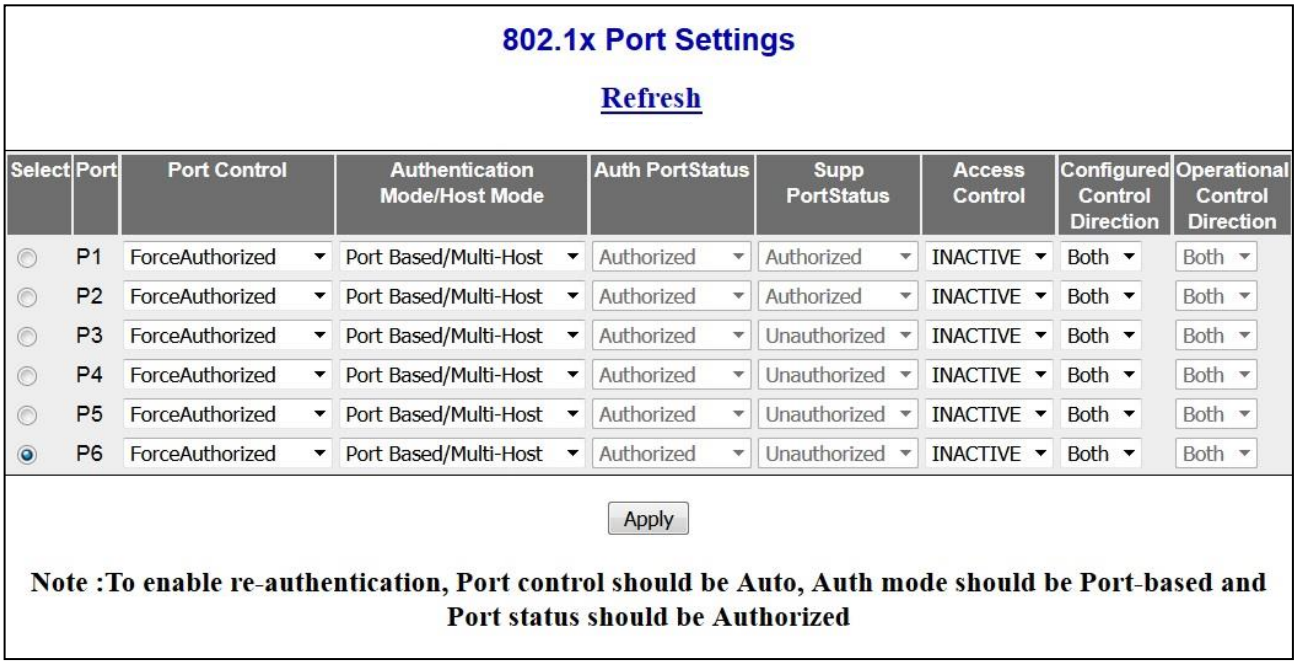


Figure 23-3 : 802.1x Port Settings Part A

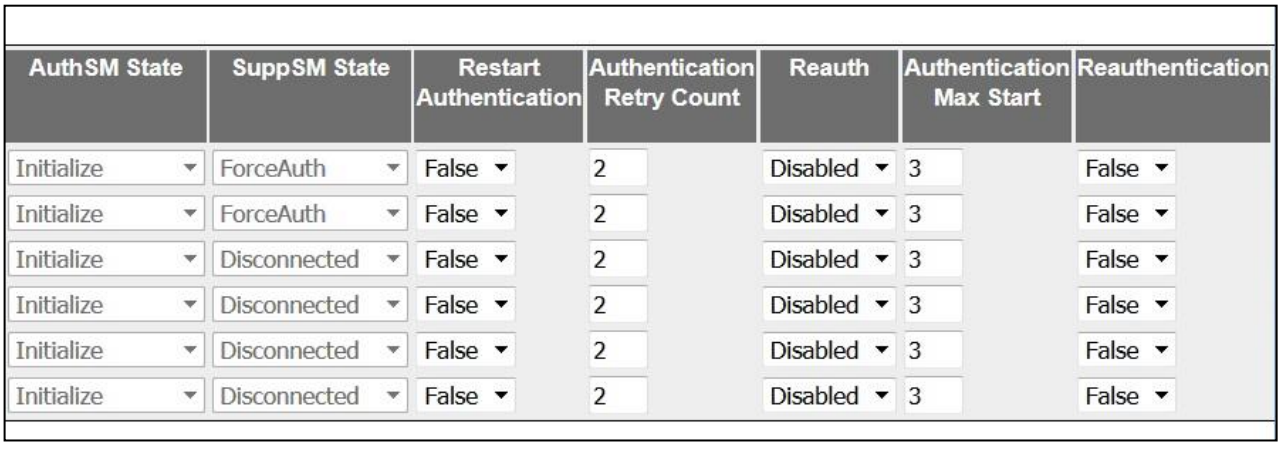


Figure 23-4 : 802.1x Port Settings Part B

Screen Objective	This screen allows the user to configure the security information at the individual port levels
Navigation	**Layer2 Management** > **802.1x** > **Port Settings**
Fields	• **Select** - Select the port for which the configuration needs to be done • **Port** - Displays the port number.

- **Port Control** - Select the control values of the Authenticator Port. The Default option is **ForceAuthorized** The options are:
  - **ForceAuthorized** – Allows all the traffic through this port. Disables 802.1X authentication and causes the port to transit to the authorized state without requiring authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client.
  - **ForceUnauthorized** – Blocks all the traffic through this port. Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.
  - **Auto** – Imposes 802.1x authentication process in this port. Causes the port to begin the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server.

- **Authentication Mode/Host Mode** - Select the authentication mode to be imposed on the entry. The Default option is Port Based. The list contains:
  - **Port Based/Multi-Host** – Authenticates and authorizes devices attached to a Bridge port that has point-to-point connection characteristics named as Port based network access control. The following occurs when Port based authentication is selected
    - Receives incoming tagged/untagged data/control frames from the CFA Module (Interface Manager) and checks if the Port is authorized. If authorized, the frame is passed to the higher layer.
    - Receives outgoing data/control frames from the other modules. If authorized, the frame is passed to the CFA module.
    - When an EAPOL frame is received from CFA, it sends the EAP packet to the PNAC Interface Task, which then passes it to the Authenticator Module or Supplicant Module.
    - It forwards all the received EAPOL-Start, EAPOL-Logoff and EAP-Responses to the Authenticator Module via the PNAC Interface Task.
    - It forwards all the received EAP-Requests, EAP-Success and EAP-Failure to the Supplicant Module via the PNAC Interface Task.
    - It forwards all the received EAPOL-Key frames to the Key Handler Module via the PNAC Interface Task.
    - It maintains the physical link status information provided by CFA and informs the Authenticator and Supplicant modules to take the necessary action on physical link UP/DOWN conditions.
    - It forms an EAPOL frame when requested by the Authenticator Module or Supplicant Module or Key Handler Module and transmits it to CFA.
  - **Mac Based/Single-Host** – Authenticates and authorizes devices attached to a Bridge port in the shared LAN named as MAC based

network access control. The following occurs when Mac based authentication is selected.

- On receiving tagged/untagged data/control frames from the CFA Module, it checks if the source MAC is present in the Authenticator Session Table and is authorized.
- If it is present in the table and is authorized, the result is passed to CFA, which then forwards the frame to the appropriate destination module.
- If it is present in the table but not authorized, the CFA Module is intimated and the frame is dropped at the CFA Module.
- If neither of the above occurs, the Authenticator will initiate a new authentication session for that source MAC address and return the unauthorized status to the CFA Module, which then drops the frame

MAC based authentication can be configured only if the Port control is Auto.

- **Auth Port Status** - Displays the status of the Authenticator Port. The options are:
  - **Authorized –** Module is ready for transmission or reception of data
  - **Unauthorized** - Module is not ready for transmission or reception of data
- **Supp Port Status** - Displays the status of the Supplicant PAE state machine. The options are:
  - **Authorized** - Module is ready for transmission or reception of data
  - **Unauthorized** - Module is not ready for transmission or reception of data
- **Access Control** - Select the Access Control status for the port. This setting is for the application of the Supplicant authorization state when the port is operating as both Supplicant and Authenticator. The default option is **INACTIVE**. The list contains:
  - **INACTIVE –** Indicates that the port uses only the Authenticator authorization state to restrict access to the port and not the Supplicant authorization state.
  - **ACTIVE –** Indicates that the port applies both the Supplicant authorization state and Authenticator authorization state.

Access Control cannot be set as ACTIVE when **Authentication Mode/Host Mode** is set as **Mac Based/Single Host**

- **Authentication Mode** - Select the authentication mode to be imposed on the entry. The The default value is **Port Based**. The options are:
  - **Port Based –** To authenticate and authorize devices attached to a Bridge port that has point-to-point connection characteristics named as Port based network access control. The following occurs when Port based authentication is selected
    - Receives incoming tagged/untagged data/control frames from the CFA Module (Interface Manager) and checks if the Port is authorized. If authorized, the frame is passed to the higher layer.

- Receives outgoing data/control frames from the other modules. If authorized, the frame is passed to the CFA module.
- When an EAPOL frame is received from CFA, it sends the EAP packet to the PNAC Interface Task, which then passes it to the Authenticator Module or Supplicant Module.
- It forwards all the received EAPOL-Start, EAPOL-Logoff and EAP-Responses to the Authenticator Module via the PNAC Interface Task.
- It forwards all the received EAP-Requests, EAP-Success and EAP-Failure to the Supplicant Module via the PNAC Interface Task.
- It forwards all the received EAPOL-Key frames to the Key Handler Module via the PNAC Interface Task.
- It maintains the physical link status information provided by CFA and informs the Authenticator and Supplicant modules to take the necessary action on physical link UP/DOWN conditions.
- It forms an EAPOL frame when requested by the Authenticator Module or Supplicant Module or Key Handler Module and transmits it to CFA

– **Mac Based** – To authenticate and authorize devices attached to a Bridge port in the shared LAN named as MAC based network access control. The following occurs when Mac based authentication is selected.

- On receiving tagged/untagged data/control frames from the CFA Module, it checks if the source MAC is present in the Authenticator Session Table and is authorized.
- If it is present in the table and is authorized, the result is passed to CFA, which then forwards the frame to the appropriate destination module.
- If it is present in the table but not authorized, the CFA Module is intimated and the frame is dropped at the CFA Module.
- If neither of the above occurs, the Authenticator will initiate a new authentication session for that source MAC address and return the unauthorized status to the CFA Module, which then drops the frame


MAC based authentication is enabled only if the **Port control** is **Auto**.

- **Configured Control Direction** - Select the value of the administrative controlled directions parameter for the port. The options are:
  - **Both** - Authentication control is imposed on both the incoming and outgoing packets
  - **In** - Authentication control is imposed on the incoming packets
- **Operational Control Direction** - Select the value of the operational controlled directions parameter for the port. The options are:
  - **Both** - Authentication control is imposed on both the incoming and outgoing packets
  - **In** - Authentication control is imposed on the incoming packets

- **Auth SM State** - Select the state of the Authenticator State Machine for the entry. The options are:
  - **Initialize** –This state occurs when the module is disabled and port is down
  - **Disconnected** – There will be a transition from Initialize to disconnecting. State Machine never remains in this state and there will be an immediate transition.
  - **Connecting** – This state is the beginning of the PNAC packet exchange
  - **Authenticating** – This state occurs whenever authenticator receives response ID from supplicant
  - **Authenticated** - This state occurs whenever authenticator SM port transitions to authorized through EAP exchange
  - **Aborting** – This state occurs when Authenticator SM receives re-authenticating event or EAP start or supplicant log off
  - **Held** - This state occurs when authentication failure occurs due to wrong user name or password
  - **ForceAuth** – This state occurs when the port control is changed to force authorized
  - **ForceUnauth** – This state occurs when the port control is changed to force unauthorized
- **SuppSMState** - Select the state of the Supplicant State Machine. The options are:
  - **Disconnected** - There will be a transition from Initialize to disconnecting. State Machine never remains in this state and there will be an immediate transition.
  - **Logoff** - State Machine never remains in this state and there will be an immediate transition to the other state
  - **Connecting** - This state is the beginning of the PNAC packet exchange
  - **Authenticating** – This state occurs whenever supplicant receives a request or challenge from authenticator
  - **Authenticated** - This state occurs whenever Supplicant SM port transitions to authorized through EAP exchange
  - **Acquired** – This state occurs whenever supplicant receives a request ID from authenticator
  - **Held** - This state occurs when authentication failure occurs due to wrong user name or password
  - **ForceAuth** – This state occurs when the port control is changed to force authorized
  - **ForceUnauth** – This state occurs when the port control is changed to force unauthorized
- **Restart Authentication** - Select the initialization control for the port to restart authentication. The options are:
  - **True** – Causes the Port to be initialized.
  - **False** – Reverts to False once initialization is complete.

This field cannot be set as True when **Authentication Mode/Host Mode** is set as **Mac Based/Single Host**

- **Authentication Retry Count** - Enter the maximum number of authentication requests that can be sent from the authenticator before getting response from the supplicant. This value ranges from 1 to 10. The default value is **2**.
- **Reauth** - Select the re-authentication mechanism on the port. It re-authenticates the port without waiting for the configured number of seconds between re-authentication attempts and automatic re-authentication. The default option is **Disabled**. The options are:
  - **Enabled** – Enables re-authentication on the port
  - **Disabled** – Disables re-authentication on the port
- **Authentication Max Start** - Enter the maximum number of successive EAPOL-Start messages that will be sent before the supplicant assumes that there is no authenticator present. This value ranges from 1 to 65535. The default value is **3**.
- **Reauthentication** - Select the re-authentication mechanism on the port. It re-authenticates the port without waiting for the configured number of seconds between re-authentication attempts and automatic re-authentication. is The default value is **False**. The list contains:
  - **True** – Enables re-authentication on the port
  - **False** – Disables re-authentication on the port

  To enable re-authentication, Port control should be Auto, Auth mode should be Port-based and Port status should be Authorized

Buttons	**Apply** - To modify attributes for the selected entry and save the changes.

23.3 802.1X Timer Configuration

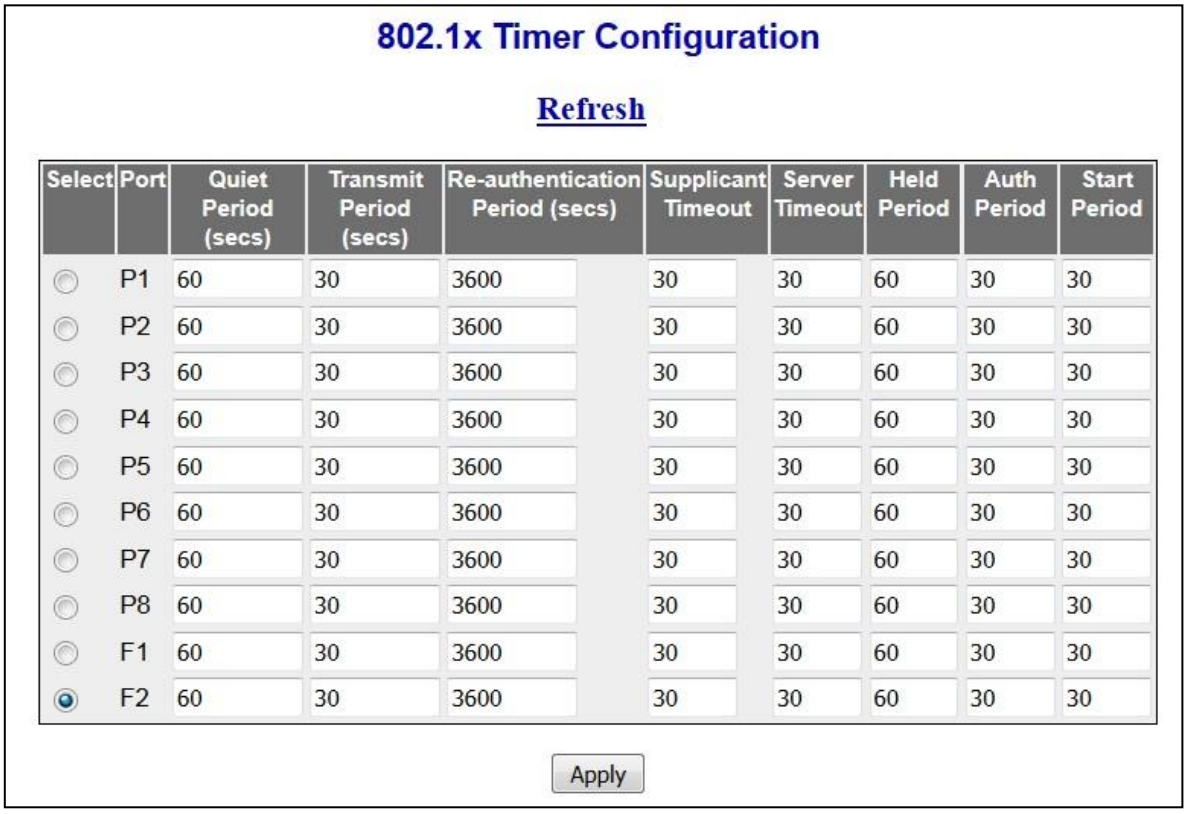


Figure 23-5 : 802.1x Timer Configuration

Screen Objective	This screen allows the user to configure the Timer parameters at the individual port level.
Navigation	**Layer2 Management** > **802.1x** > **Timers**
Fields	• **Port** - Displays the number. • **Quiet Period (secs)** - Enter the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. In this the duration the authenticator remains silent and will not attempt to acquire a supplicant. This value ranges from 0 to 65535 seconds. The default value is **60** seconds. • **Transmit Period (secs)** - Enter the Time Period used by the Authenticator State machine to define when the EAP Request ID PDU is to be transmitted. This value ranges from 1 to 65535 seconds. The default value is **30** seconds. • **Re-authentication Period (secs)** - Enter the time between periodic re-authentication of the supplicant. Re-authentication period denotes the number of times the switch restarts the authentication process before the

port changes to the unauthorized state. This value ranges from 1 to 65535 seconds. The default value is **3600** seconds.

- **Supplicant Timeout** - Enter the amount of time the switch waits for a response before resending the request to the client, when relaying a request from the authentication server to the client. This value ranges from 1 to 65535 seconds. The default value is **30** seconds.
- **Server Timeout** - Enter the amount of time the switch waits for a reply before resending the response to the server, when relaying a response from the client to the authentication server. This value ranges from 1 to 65535 seconds. The default value is **30** seconds.
- **Held Period** - Enter the amount of time the client will wait before re-attempting a failed 802.1X authentication. When the Supplicant (in the client) receives an authentication failure indication from the Switch, it remains idle for a period of time which is determined by the value of held-period. After this time, the supplicant initiates authentication again. Authentication failure might occur if supplicant provides a wrong password. This value ranges from 1 to 65535 seconds. The default value is **60**.
- **Auth Period** - Enter the time interval for resending 802.1X request messages after not receiving a response. This value ranges from 1 to 65535 seconds. The default value is **30** seconds.
- **Start Period** - Enter the time interval for resending Start messages. Start period denotes the number of seconds between successive EAPOL-Start messages following no response from the authenticator. This value ranges from 1 to 65535 seconds. The default value is **30** seconds.

Buttons	**Apply** - To modify attributes for the selected entry and save the changes.

23.4 802.1x Local Authentication Server Configuration

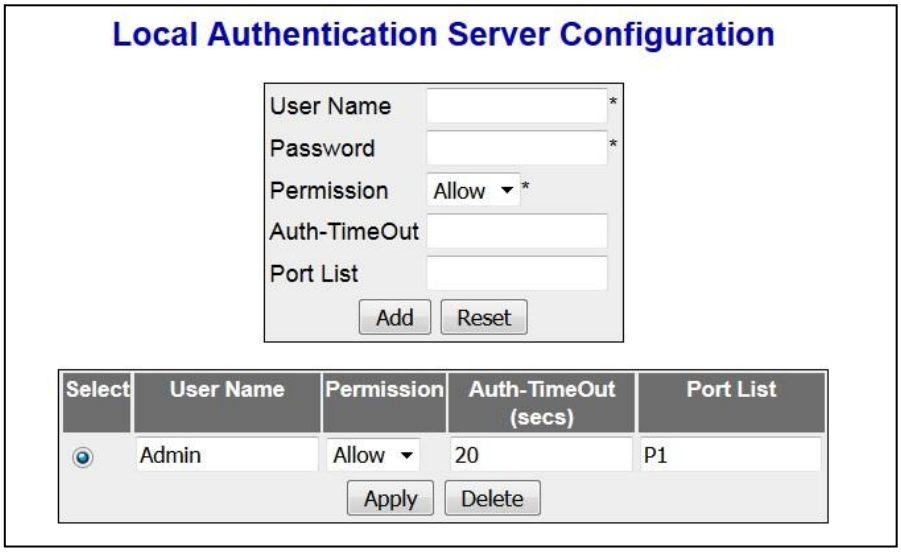


Figure 23-6 : 802.1x Local Authentication Server Configuration

Screen Objective	This screen allows the user to configure the Local Authentication Server information. It contains authentication related User configuration information maintained by PNAC local Authentication Server. Each entry contains User name, Password, Authentication protocol used, Authenticated session timeout and Access ports list of the User seeking authentication
Navigation	**Layer2 Management** > **802.1x** > **Local AS**
Fields	• **User Name** - Enter the identity of the user seeking authentication. This field is a string of maximum size 20. • **Password** - Enter the password specific to the user name. This field is a string of maximum size 20. • **Permission** - Select the allowance /denial of access for local authentication server. The options are: – **Allow** - Authentication request is allowed over the set of ports in the Port List. – **Deny** - Authentication request is not allowed over the set of ports in the Port List. • **Auth-TimeOut (secs)** - Enter the Authentication Timeout in seconds. The time in seconds after which the Authentication offered to the User ceases. When the object value is 0, the ReAuthPeriod of the Authenticator port is used by Authenticator. This value ranges from 1 to 7200 seconds. • **Port List** - Enter the complete set of ports of the authenticator to which the user is allowed or denied access, based on the Permission.

Buttons	• **Add** - To add and save new configuration. • **Reset** - To reset to default value for respective fields and discard all user inputs. • **Apply** - To modify attributes for the selected entry and save the changes. • **Delete** - To delete the selected entry.

23.5 802.1x RADIUS Server Configuration

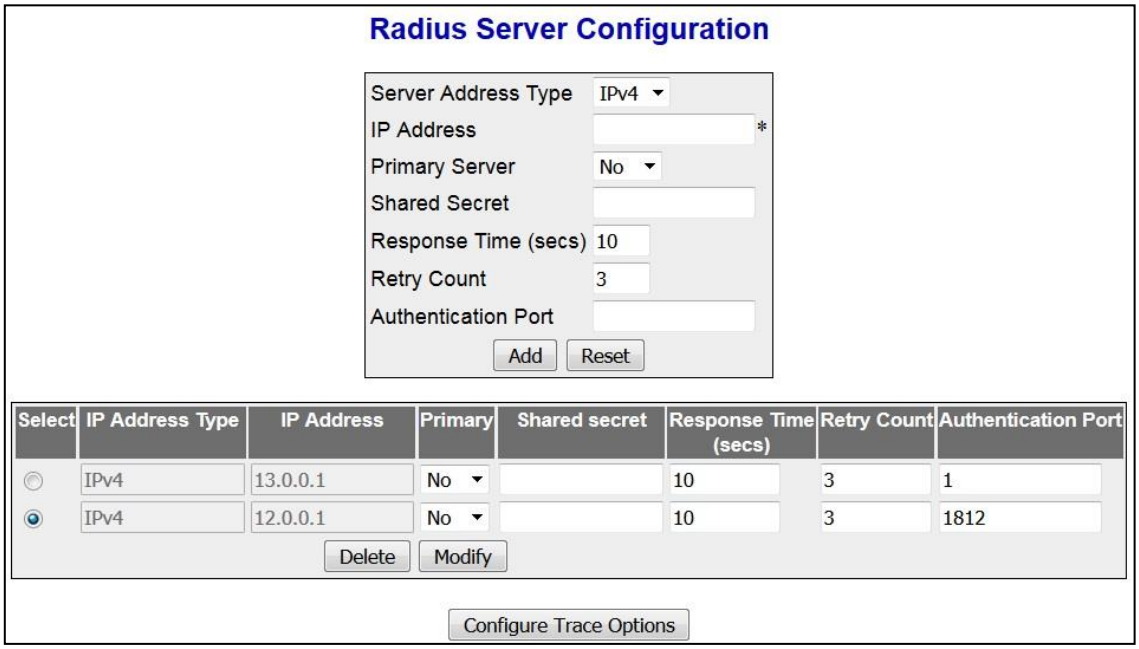


Figure 23-7 : 802.1x Radius Server Configuration

Screen Objective	This screen allows the user to configure the Radius Server settings RADIUS is a portable implementation of the RADIUS client protocol. This protocol carries authentication information between the Network Access Server (NAS) that desires to authenticate its links and the RADIUS server that is responsible for authenticating and maintaining the authentication information
Navigation	**Layer2 Management > 802.1x > Radius Settings**
Fields	• **Server Address Type** - Select the Radius server address type. The default option is **IPV4**. Options are: – **IPV4** – Radius server address type is set as Internet Protocol Version 4, where a 32 bit address is used. – **IPV6** - Radius server address type is set as Internet Protocol Version 6, where a 128 bit address is used. • **IP Address** - Enter the IP Address of the Radius Server. • **Primary Server** - Select server type. is a primary server or not. Only one server can be configured as the primary server. . The default option is **No**. Options are: – **Yes** – Indicates the server type as primary server. – **No** – Indicates the server type is not primary server. • **Shared Secret** - Enter the secret string, which is to be shared between the Radius Server and the Radius Client. The shared secret is the secret of

	the server to which the request was sent and from which the response was received. • **Response Time (secs)** - Enter the maximum time within which the Radius Server is expected to respond for a request from the Radius Client. This value ranges from 1 to 120 seconds. The default value is **10**. • **Retry Count** - Enter the maximum number of times a request can be re-transmitted before getting response from the Radius Server. If the retransmit count has exceeded the configured maximum retransmissions, the packet and the user entry are deleted from the user request table and the error condition is logged. This value ranges from 1 to 254. The default value is **3**. • **Authentication Port** – Enter the port number used for authentication. This value ranges from 1 to 65535.
Buttons	• **Add** - To add and save new configuration. • **Reset** - To reset to default value for respective fields and discard all user inputs. • **Modify** - To modify attributes for the selected entry and save the changes. • **Delete** - To delete the selected entry. • **Configure Trace Options** - To access **Radius Traces** screen

23.5.1 802.1x RADIUS Traces

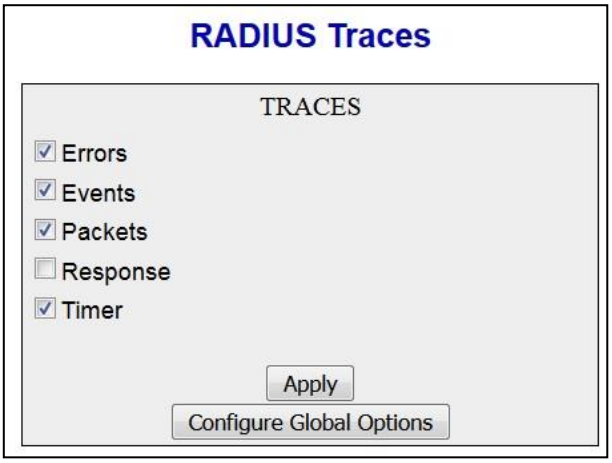


Figure 23-8 : 802.1x Radius Traces

Screen Objective	This screen allows the user to enable the required debug statements that are useful during debug operation. A FOUR BYTE integer is used for enabling the level of tracing. Each BIT in the four byte integer represents a particular level of Trace. Combination of levels is also allowed. System errors such as memory allocation failures are notified by means of LOG messages and TRACE messages. Interface errors and protocol errors are notified by means of TRACE messages
Navigation	**Layer2 Management > VLAN > 802.1x > Radius Settings> Radius Server Configuration** screen **>** click **Configure Trace Options** button
Fields	• **Traces** - Select the traces for which debug statements is to be generated. The options are – **Error** - Generates debug statements for all failure traces of the below mentioned traces. – **Events** - Generates event debug statements. Generates debug statements for event handling traces. This trace is generated for event processing or response occurring with respect to radius – **Packets** - Generates packet debug statements. Generates debug statements for packets handling traces. This trace is generated for packet transmission or reception scenarios. – **Response** - Generates response debug statements. This trace provides information about the response from the Radius server – **Timer** - Generates timer debug statements. This trace is generated for timer functionality.

Buttons	• **Apply** - To modify attributes and save the changes. • **Configure Global Options** - To return to the **Radius Server Configuration** screen

23.6 802.1x MAC Session Info

Figure 23-9 : 802.1x Mac Session Info

Screen Objective	This screen displays the MAC Session information details. It contains authentication session information associated with each Supplicant while Authenticator operates in MAC based authentication mode. The MAC session entries are deleted from the port whenever it receives the port operational status down information
Navigation	**Layer2 Management > 802.1x > MacSession Info**
Fields	• **Supplicant MacAddr** - Displays the Supplicant MAC Address for the session. • **Session Identifier** - Displays the Session Identifier of the supplicant for the session. • **Auth SM State** - Select the state of the Authenticator State Machine for the entry. The list contains: – **Initialize** –This state occurs when the module is disabled and port is down – **Disconnected** – There will be a transition from Initialize to disconnecting. State Machine never remains in this state and there will be an immediate transition. – **Connecting** – This state is the beginning of the PNAC packet exchange – **Authenticating** – This state occurs whenever authenticator receives response ID from supplicant – **Authenticated** - This state occurs whenever authenticator SM port transitions to authorized through EAP exchange – **Aborting** – This state occurs when Authenticator SM receives re-authenticating event or EAP start or supplicant log off

- **Held** - This state occurs when authentication failure occurs due to wrong user name or password
- **ForceAuth** – This state occurs when the port control is changed to force authorised
- **ForceUnauth** - This state occurs when the port control is changed to force unauthorised

- **Auth Session Status** - Displays the Authentication Session Status.
  - **Authorized** – Module is ready for transmission or reception of data
  - **Unauthorized** - Module is not ready for transmission or reception of data
- **Session PortNumber** - Displays the port number through which a particular Session MAC address is learnt.
- **Session Initialize** – Select the session initialize status for the supplicant mac address configured. The default value is True. This list contains;
  - **True** – Indicates session initialize is set
  - **False** - Indicates session initialize is reset
- **Session Reauthenticate** - Select the session reathentication status for the supplicant mac address configured. The default value is True. This list contains;
  - **True** – Indicates session re-authentication is initialized
  - **False** - Indicates session re-authentication is reset

Buttons	**Apply** - To modify attributes for the selected entry and save the changes

Chapter 23

IP Management

IP (Internet Protocol) is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. Example: 10.5.25.180.

Every computer that communicates over the Internet is assigned an IP address that uniquely identifies the device and distinguishes it from other computers on the Internet. Within an isolated network, IP addresses can be assigned at random as long as each one is unique. However, to connect a private network to the Internet, the registered IP addresses must be used (called Internet addresses) to avoid duplicates. The four numbers in an IP address are used in different ways to identify a particular network and a host on that network.

Four regional Internet registries -- ARIN, RIPE NCC, LACNIC and APNIC -- assign Internet addresses from the following three classes.

- Class A - supports 16 million hosts on each of 126 networks
- Class B - supports 65,000 hosts on each of 16,000 networks
- Class C - supports 254 hosts on each of 2 million networks

The number of unassigned Internet addresses is running out, so a new classless scheme called CIDR (Classless Inter-Domain Routing) is gradually replacing the system based on classes A, B, and C and is tied to adoption of IPv6.

ICMP (Internet Control Message Protocol) is an extension to the IP defined by RFC 792. ICMP supports packets containing error, control, and informational messages. For example the ping command uses ICMP to test an Internet connection.

IP (Internet Protocol) functions at the network layer. IP delivers/forwards packets to the higher layer and to other hosts/routers. The forwarding table maintained by IP consists of the Static Routers and the Routes learnt from other Routing Protocols.

To access **IP** screens, click **IP Management > IP**

The **IP** related parameters are configured through the screens displayed by the following tabs:

- IPv4 Interface Settings
- IPv4 IP Route Configuration

24.1 IPv4 Interface Settings

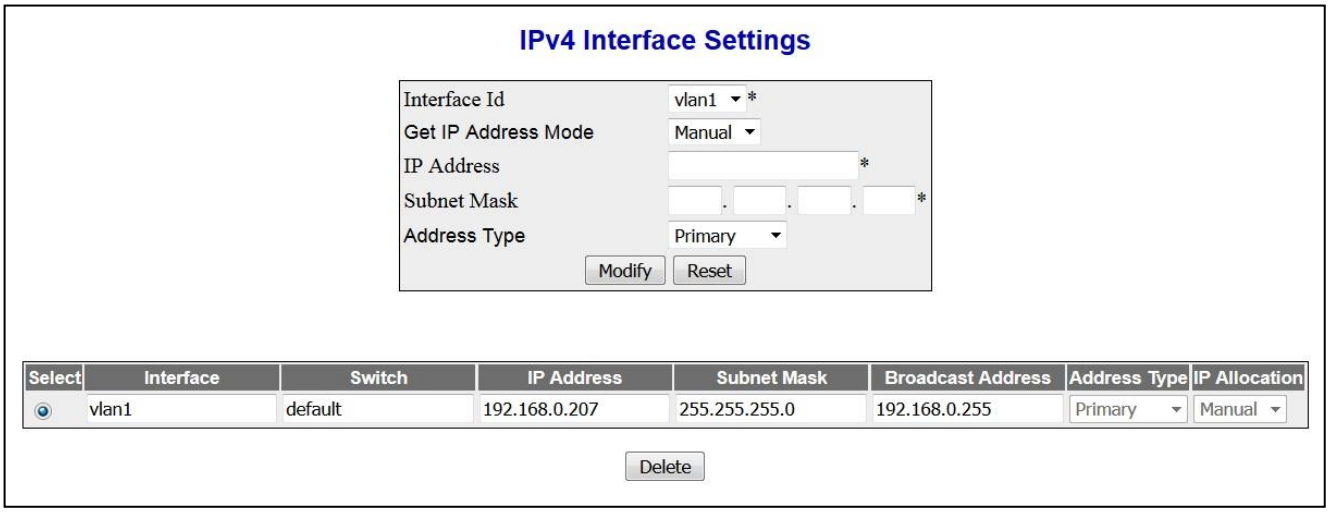


Figure 24-1 : IPv4 Interface Settings

Screen Objective	This screen allows the user to configure the settings of the IPv4 interface
Navigation	**IP Management** > **IP** > **IP Address Configuration**

- **Select** - Select the VLAN Interface for which the configurations need to be deleted.
- **Interface** - Select the index value which uniquely identifies the VLAN interface to which this entry is applicable.
- **Get IP Address Mode / IP Allocation** - Select the protocol to be used to obtain the IP address from the interface. The default option is **RARP.** The list contains:

- **Manual** - Configures the IP address manually to a specified address by the user or administrator.
- **RARP** - Assigns the IP address to the system by a RARP (Reverse Address Resolution Protocol) server.
- **DHCP** - Assigns the IP address to the system by a DHCP (Dynamic Host Configuration Protocol) server. DHCP-client tries for dynamic IP address from server for maximum number of retries. If not successful in receiving any IP address, then rolls back to default IP address

- **Switch** - Specifies the name of the switch context.
- **IP Address** - Enter the IP Address of the interface. If the interface is not a network interface then the default value of 0.0.0.0 is assigned and the interface is treated as a non-numbered interface by IP.
- **Subnet Mask** - Enter the subnet mask for the provided IP address.
- **Broadcast Address** - Displays the broadcast address for the specified IP address.
- **Address Type** - Select the type of IP address for the specified VLAN interface.. The default option is **Primary.** The list contains:
  - **Primary** - Sets the address type as Primary IP address for the specified interface
  - **Secondary** - Sets the address type as secondary IP address this is an additional IP address that can be configured for the specified interface.

  The secondary IP address can be created only if the primary IP address is already created for the interface.

Buttons

- **Modify** - To add and save new configuration
- **Reset** - To reset to default value for respective fields and discard all user inputs
- **Delete** - To delete the selected entry.

24.2 IPv4 IP Route Configuration

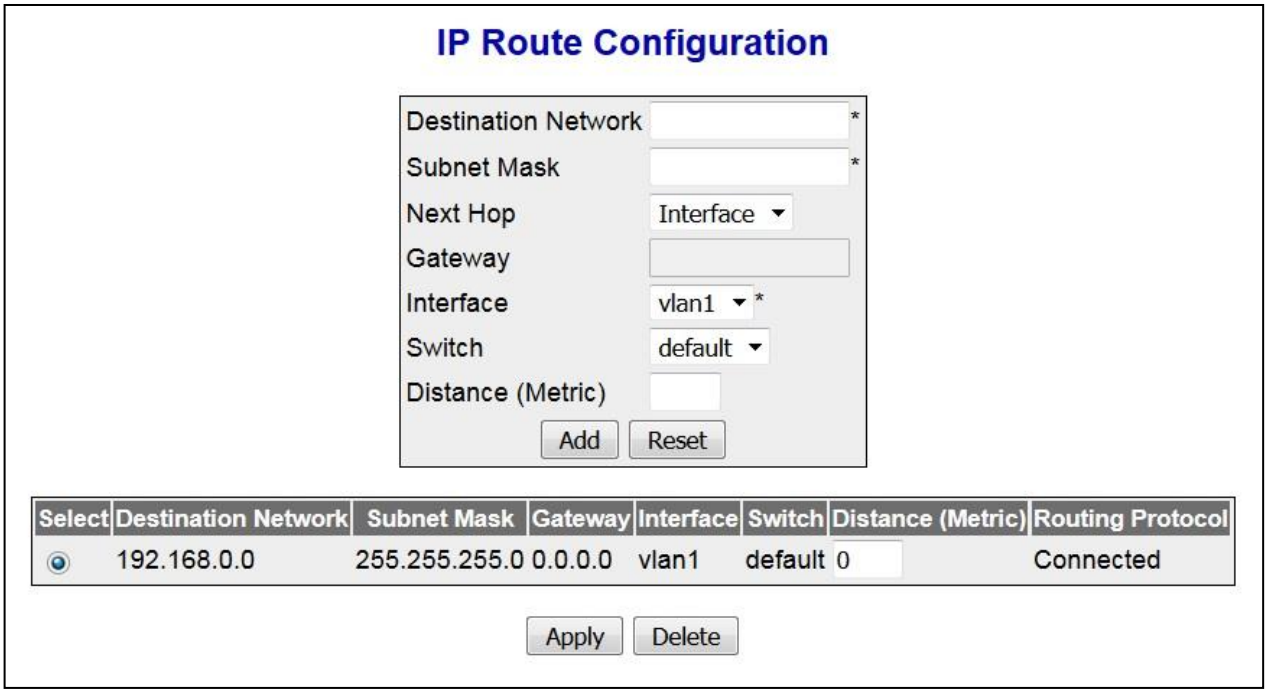


Figure 24-2 : IPv4 IP Route Configuration

Screen Objective	This screen allows the user to configure IP route information
Navigation	**IP Management** > **IP Route Configuration**
Fields	• **Select** - Select the destination network for which the configurations need to be modified or deleted. • **Destination Network** - Enter the destination IP address of the route. It denotes the Network Address for which the route is being added. • **Subnet Mask** - Enter the subnet mask for the Destination Network address. • **Gateway** - Enter the Next Hop gateway to reach the Destination Network. • **Interface** - Select the outgoing interface through which the Destination Network is reachable. • **Switch** - Specifies the name of the switch context. • **Distance (Metric)** - Enter the Metric value of the destination. The semantics of this metric are determined by the routing-protocol. The value ranges from 1 to 255. The default value is **1**.

- **Routing Protocol** - Displays the status of the routing protocol through which the route was learnt, if the route is not a directly connected network or a static route.

Buttons

- **Add** - To add and save new configuration
- **Reset** - To reset to default value for respective fields and discard all user inputs
- **Apply** - To modify attributes for the selected entry and save the changes

  Only static routes can be deleted or modified

- **Delete** - To delete the selected entry

Example : Gateway

The following screenshot example shows the result of an IP Gateway route having being configured.

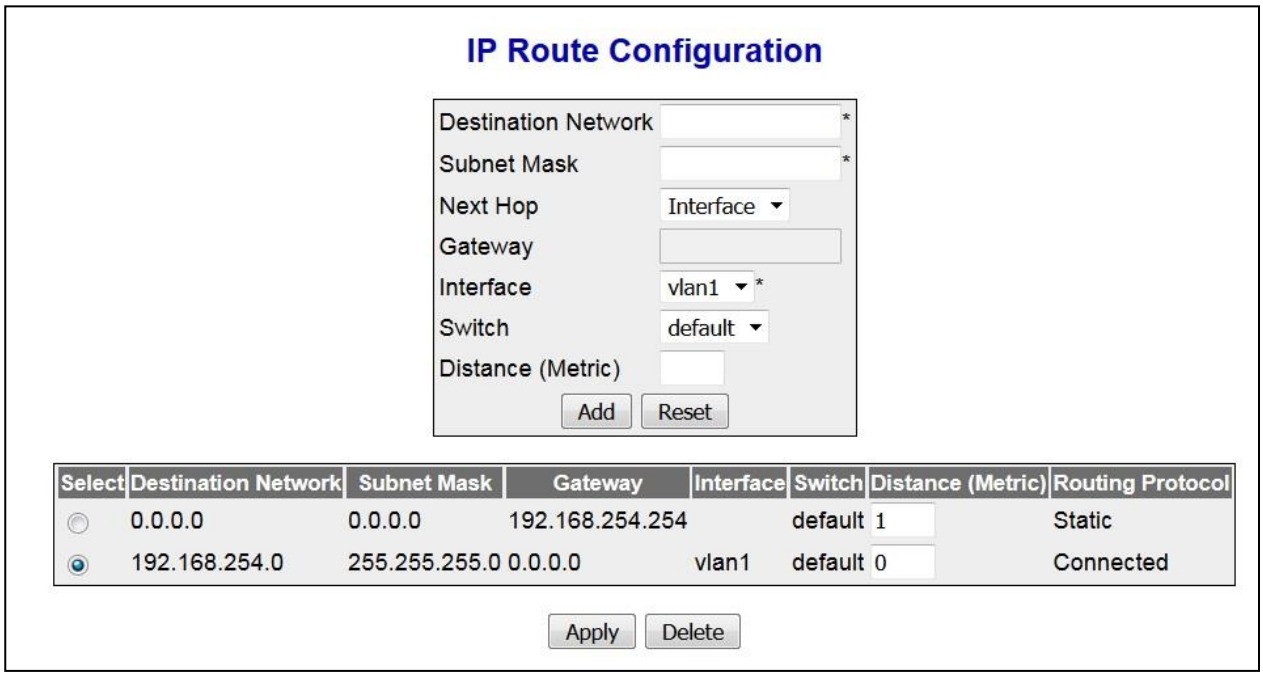


Figure 24-3 : IPv4 IP Route Configuration : Gateway

Chapter 24

DHCP Server

DHCP (Dynamic Host Configuration Protocol) is used in a wide variety of devices like ISDN routers, firewalls, etc., for assigning IP addresses to workstations. Besides obtaining IP address, other configuration parameters for a workstation can also be configured in a DHCP server. DHCP clients can retrieve these parameters along with the IP address.

DHCP is based on the client-server architecture. DHCP servers are configured with an IP address and several other configuration parameters. DHCP clients, typically workstations obtain this IP address at start-up. The client obtains the address for a time period termed as the “lease” period. DHCP clients renew the address by sending a request for the IP address before the lease expires.

DHCP uses UDP as its transport protocol and a UDP port for communication. DHCP relay Agents connect servers present on one LAN with the client present on another.

DHCP server is responsible for dynamically assigning unique IP address and other configuration parameters such as gateway, to interfaces of a DHCP client. The IP address is leased to the interface only for a particular time period as mentioned in the DHCP lease. The interface should renew the DHCP lease once it expires. The DHCP server contains a pool of IP address from which one address is assigned to the interface.

To access **DHCP** screens, click **IP Management > DHCP Server**.

The **DHCP Server** related parameters are configured through the screens displayed by the following tabs:

- Basic Settings
- Pool Settings
- Pool Options
- Exclude List
- Host Settings
- Host Options
- DHCP Pool Options : Appendix A

By default, the tab **DHCP Server** displays the **DHCP Basic Settings** screen.

25.1 DHCP Basic Settings

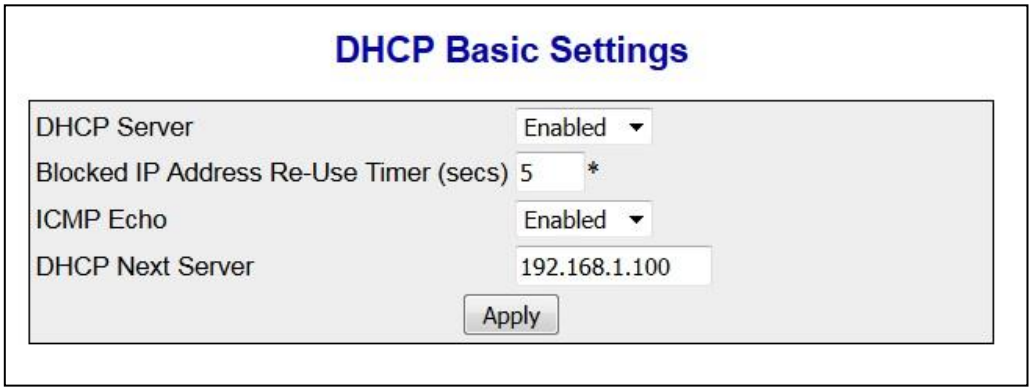


Figure 25-1: DHCP Basic Settings

Screen Objective	This screen allows the user to configure the basic DHCP settings.
☞	To enable DHCP Server, DHCP Relay Status should be disabled.
Navigation	**IP Management > DHCP Server > Basic Settings**
Fields	• **DHCP-Server** - Select the DHCP server status in the router.The default option is **Disabled**. The list contains: – Enabled - Enables the DHCP server in the router and starts serving the server with the IP addresses. It opens the UDP socket and starts listening for DHCP discover messages from clients. – Disabled - Disables the DHCP server in the router. • **Blocked IP Address Re-Use Timer (secs)** - Enter the reuse timeout value used by DHCP in seconds. It denotes the amount of time the DHCP server entity waits for the DHCP REQUEST from the client, before reusing the offer, like the blocked IP address. The value zero disables this timer.This value ranges from 1 to 120 seconds. The default value is **5** seconds. • **ICMP Echo** - Select the status of ICMP (Internet Control Message Protocol) Echo feature for the DHCP server.. This object controls the server to probe for the IP address before allocating the IP address to a client through the ICMP echo message. The default option is **Disabled**. The list contains: – Enabled - Enables the ICMP Echo feature. Before allocating an IP Address to client, the server broadcasts ICMP Echo Request (Ping Packet) to check whether any other machine/host is using this IP. If there is no response received, the server allocates the IP to the client. – Disabled - Disables the ICMP Echo feature. The ICMP Echo Request packet mechanism is not used. The IP is directly allocated to the client • **DHCP Next Server -** Sets the IP address of the boot server (TFTP server) from which the initial boot file is to be loaded in a DHCP client. This

	boot server acts as a secondary server. The default address is 0.0.0.0 (No boot server is defined. DHCP server is used as the boot server
Buttons	**Apply** - To modify the attributes and save the changes. **Delete** - To delete the selected entry

25.2 DHCP Pool Settings

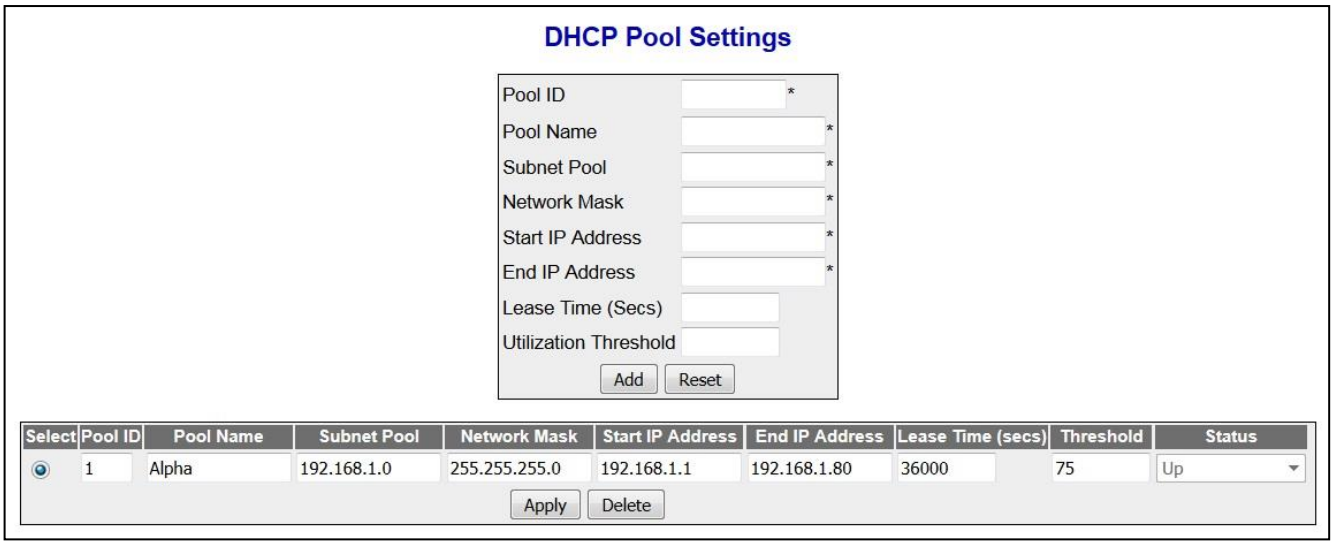


Figure 25-2: DHCP Pool Settings

Screen Objective	This screen allows the user to configure the DHCP address pool. DHCP address pools are used by the servers to allocate the IP addresses to the clients.
Navigation	**IP Management** > **DHCP Server** > **Pool Settings**
Fields	• **Select -** Click to select pool id for which the configuration needs to be modified or deleted. • **Pool ID** - Enter the pool Identifier. This is unique index for each subnet pools. This value ranges from 1 to 2147483647. • **Pool Name** - Enter the pool name to identify the subnet pool. This is a string of maximum size 64. • **Subnet Pool** - Enter the subnet of the IP address in the pool. • **Network Mask** - Enter the network mask. It denotes the client's subnet mask of the IP address in the pool.

- **Start IP Address** - Enter the first IP address in the address pool that is used for dynamic allocation by the DHCP server. This specifies the lower limit for IP address in an address pool.

  Start IP address should have same network of the subnet pools.

- **End IP Address** - Enter the last IP address in the address pool that is used for dynamic allocation by the DHCP server. This specifies the upper limit for IP address in an address pool.

  End IP address should have same network of the subnet pools.

- **Lease Time (Secs)** - Enter the time interval for which the IP address is valid. It This specifies the amount of time that the client can use the IP address assigned by the server andis specific to each IP address pool. Every IP address allocated from a pool will be returned to the pool, if the client does not renew it. This value ranges from 60 to 2147483647 seconds. The default value is **3600 seconds**.

- **Utilization threshold / Threshold** - Enter the DHCP Pool utilization threshold value in percentage. This specifies the upper limit for the address pool utilization, after which a notification will be sent to SNMP manager.This value ranges from 0 to 100 in percentage.The default value is **75**.

- **Status** - Select the status of the entry. It denotes the status of address pool configuration and allocation of IP address. Options are
  - UP - Configures the address pool successfully for allocating IP address.
  - Down - Does not configure address pool for allocating IP address.

Buttons

- **Add** - To add and save new configuration
- **Reset** - To reset to default value for respective fields and discard all user inputs
- **Apply** - To modify attributes for the selected entry and save the changes
- **Delete** - To delete the selected entry

25.3 DHCP Pool Option settings

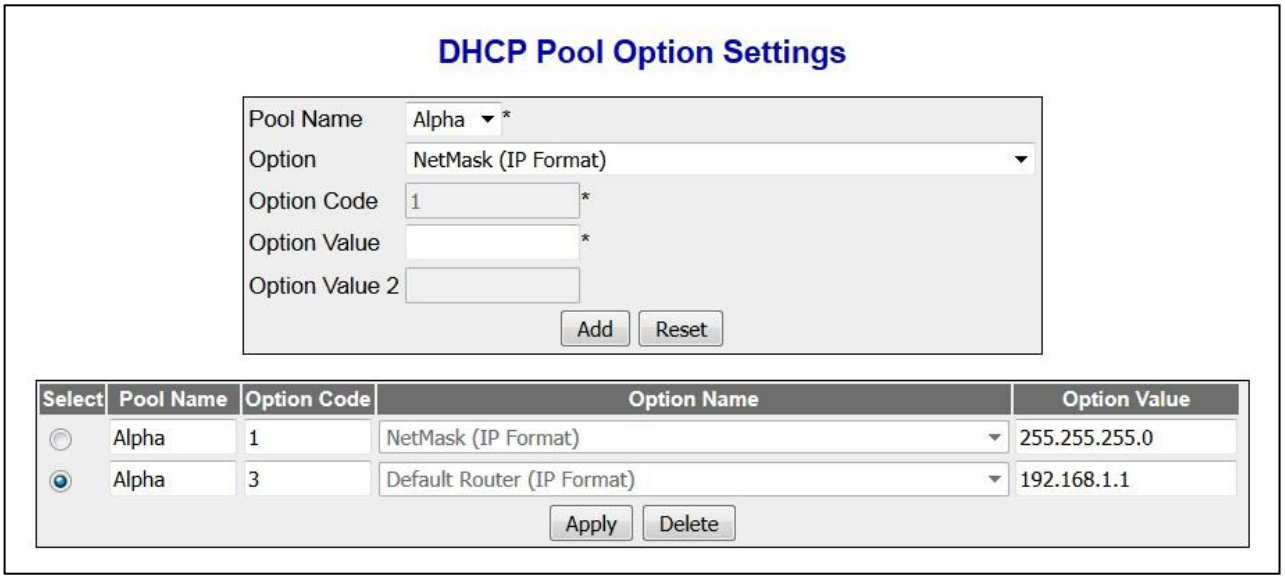


Figure 25-3: DHCP Pool Options Settings

Screen Objective	This screen allows the user to set the DHCP server pool options related configuration. The configured options are sent to DHCP client in DHCP offer packet.
☞	This screen can be configured only if Pool is created using **DHCP Pool settings** screen.
Navigation	**IP Management** > **DHCP Server > Pool Options**
Fields	• **Select -** Click to select pool name for which the configuration needs to be modified or deleted. • **Pool Name** - Select the pool name from the list of Address Pools created in the system for which DHCP pool options related configuration needs to be applied. ✎ This field lists the pool names created in **DHCP Pool settings** screen • **Option / Option Name** - Select the DHCP pool option that is to be set to the selected pool name. The default option is **NetMask (IP Format)** . ✎ Refer to DHCP Pool Options: Appendix A for the items in the list and their description. • **Option Code** - Displays the corresponding DHCP option code for the DHCP option selected in the field **option**. The option code represents that represents a specific DHCP option used in a DHCP OFFER message in response to a DHCP DISCOVER message. The default option code is **1** (the code for the default option – Netmask (IP Format) .

Refer to DHCP Pool Options: Appendix A for details about option code and its corresponding DHCP option.

This field is configurable if the option is selected as “Enter Option Code Manually”.

- **Option Value** - Enter the value to be set for the DHCP option selected in the field **option**. This value can be an ASCII string, hexadecimal string or unicast IP address based on the DHCP pool option.
- Enter the value to be set for the specified DHCP option. This value can be an ASCII string, hexadecimal string or unicast IP address based on the DHCP pool option.

This field is enabled only when the **Option/Option Name** is set as **Network Time Protocol server (IP Format), SIP Server IP Format** and **SIP Server Domain name**

Buttons

- **Add** - To add and save new configuration
- **Reset** - To reset to default value for respective fields and discard all user inputs
- **Apply** - To modify attributes for the selected entry and save the changes
- **Delete** - To delete the selected entry

The entry can be deleted only after deleting the entry in **DHCP Pool settings** screen

25.4 DHCP Server IP Exclude Settings

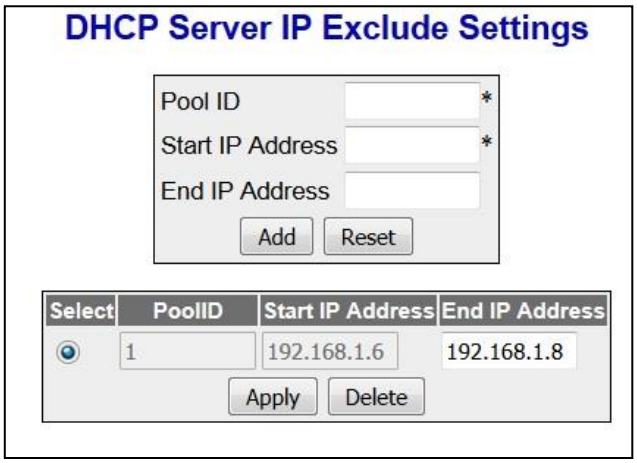


Figure 25-4: DHCP Server IP Exclude Settings

Screen Objective This screen allows the user to configure the DHCP server IP address to be excluded from the DHCP server address pool. The addresses in the created list are not allocated to the DHCP client while performing dynamic IP allocation.

Navigation	**IP Management> DHCP Server > Exclude List**
Fields	• **Select -** Click to select pool ID for which the configuration needs to be re-applied. • **Pool id** - Enter the pool ID for which exclude list is to be created. Pool ID should be created using the **DHCP Pool Settings** screen prior to configuring the exclude list. • **Start IP address** - Enter the start IP address for the exclude list. This address denotes the first IP address of a range of IP addresses which needs to be excluded from the created subnet pool. This IP address should be: • lower than the end IP address of the exclude list, and • In the same network of the subnet pool start IP address. • **End IP address** - Enter the end IP address for the exclude list. This address denotes the last IP address of a range of IP addresses which needs to be excluded from the created subnet pool. This IP address should be: • higher than the start IP address of the exclude list, and • Within or equal to the subnet pool end IP address.
Buttons	• **Add** - To add and save new configuration • **Reset** - To reset to default value for respective fields and discard all user inputs • **Apply** - To modify attributes for the selected entry and save the changes • **Delete** - To delete the selected entry

25.5 DHCP Host IP Settings

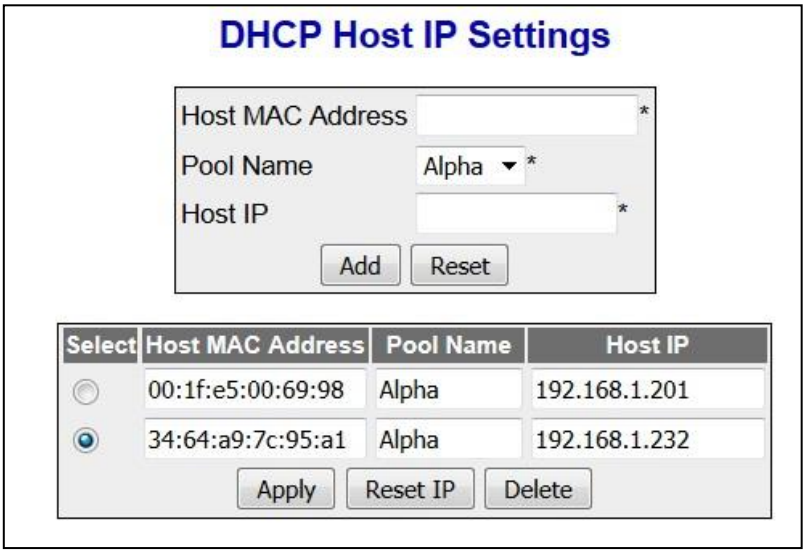


Figure 25-5: DHCP Host IP Settings

Screen Objective	This screen allows the user to configure the host IP settings.
☞	This screen can be configured only if Pool is created using **DHCP Pool settings** screen.
Navigation	**IP Management** > **DHCP Server > Host Settings**
Fields	• **Select** - Click to select MAC address for which the configuration needs to be modified or deleted. • **Host MAC Address** - Enter the unicast MAC address for configuring the DHCP host. • **Pool Name** - Select the pool name from the list of Address Pools created in the system for which DHCP host IP related configuration needs to be applied. ✎ This field lists the pool names created in **DHCP Pool settings (IP Management** > **DHCP Server** > **Pool Settings)** screen • **Host IP - Enter the IP address for** configuring the DHCP host.
Buttons	• **Add** - To add and save new configuration • **Reset** - To reset to default value for respective fields and discard all user inputs • **Apply** - To modify attributes for the selected entry and save the changes

- **Reset IP** - To reset the IP Address and discard all user inputs.
- **Delete** - To delete the selected entry

25.6 DHCP Host Option Settings

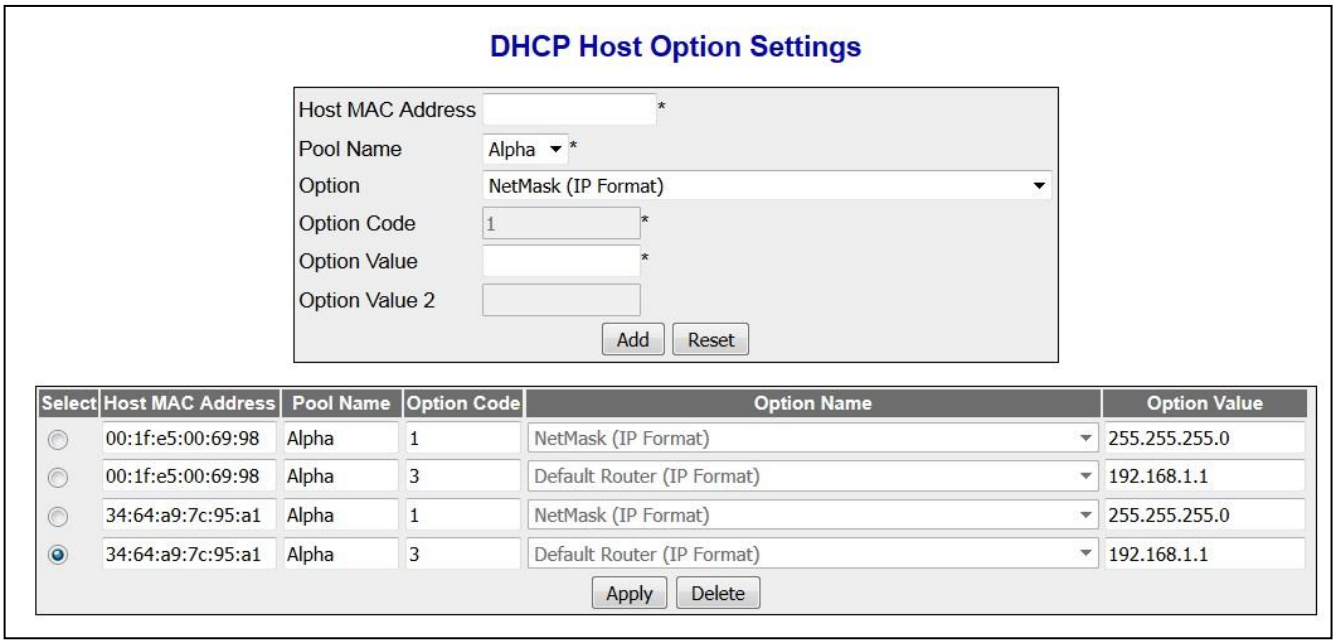


Figure 25-6: DHCP Host Option Settings

Screen Objective	This screen allows the user to configure the host option settings.
☞	This screen can be configured only if Pool is created using **DHCP Pool settings** screen.
Navigation	**IP Management> DHCP Server > Host Options**
Fields	• **Select -** Click to select Host MAC address for which the configuration needs to be re-applied. • **Host MAC Address** - Enter the unicast MAC address for configuring the DHCP host. • **Pool Name** - Select the pool name from the list for which DHCP host IP related configuration needs to be applied. ✎ This field lists the pool names created in **DHCP Pool settings screen**

- **Option/ Option Name** - Select the DHCP pool option that is to be set to the selected pool name. The default option is **NetMask (IP Format)**

  Refer to DHCP Pool Options : Appendix A for the items in the list and their description.

- **Option Code** - Displays the corresponding DHCP option code for the DHCP option selected in the field **option**. The option code represents that represents a specific DHCP option used in a DHCP OFFER message in response to a DHCP DISCOVER message The default option code is **1** (the code for the default option – **Netmask (IP Format)** .

  Refer Appendix A for details about option code and its corresponding DHCP option.

  This field is configurable if the option is selected as “Enter Option Code Manually”.

- **Option Value** - Enter the value to be set for the DHCP option selected in the field **option**. This value can be an ASCII string, hexadecimal string or unicast IP address based on the DHCP pool option.

- **Option Value 2 -** Enter the value to be set for the specified DHCP option. This value can be an ASCII string, hexadecimal string or unicast IP address based on the DHCP pool option.

  This field is enabled only when the **Option/Option Name** is set as **Network Time Protocol server (IP Format), SIP Server IP Format** and **SIP Server Domain name**

Buttons

- **Add** - To add and save new configuration
- **Reset** - To reset to default value for respective fields and discard all user inputs
- **Apply** - To modify attributes for the selected entry and save the changes
- **Delete** - To delete the selected entry

25.7 DHCP Pool Options : Appendix A

This section describes the various DHCP Server pool options and their corresponding option code.

Option	Description	Option Code
NetMask (IP Format)	Configures the client's subnet mask. The subnet mask option should be configured prior to the router option. The length is 4 octets.	1
Time Offset (Integer or Hexa (Prefix "0x" before number))	Configures the offset of the client's subnet (in seconds) from UTC (Coordinated Universal Time). A positive offset indicates a location east of the zero meridian and a negative offset indicates a location west of the zero meridian. The length is 4 octets.	2
Default Router (IP Format)	Configures a list of IP addresses for routers on the client's subnet. Routers should be listed in order of preference. The minimum length is 4 octets. The length should always be a multiple of 4.	3
Time Server (IP Format)	Configures a list of time servers available to the client. Servers should be listed in order of preference. The minimum length is 4 octets. The length should always be a multiple of 4.	4
Name Server (IP Format)	Configures a list of name servers available to the client. Servers should be listed in order of preference. The minimum length is 4 octets. The length should always be a multiple of 4.	5
Domain Name Server (IP Format)	Configures maximum of two domain name system name servers available to the client. Servers should be listed in order of preference. The minimum length is 4 octets. The length should always be a multiple of 4.	6
Log Server (IP Format)	Configures a list of MIT-LCS UDP log servers available to the client. Servers should be listed in order of preference. The minimum length is 4 octets. The length should always be a multiple of 4.	7
Cookie Server (IP Format)	Configures a list of cookie servers available to the client. Servers should be listed in order of preference. The minimum length is 4 octets. The length should always be a multiple of 4.	8
LPR Server (IP Format)	Configures a list of line printer servers available to the client. Servers should be listed in order of preference. The minimum length is 4 octets. The length should always be a multiple of 4.	9
Impress Server (IP Format)	Configures a list of image impress servers available to the client. Servers should be listed in order of preference. The minimum length is 4 octets. The length should always be a multiple of 4.	10

Option	Description	Option Code
Resource Location Server (IP Format)	Configures a list of resource location servers available to the client. Servers should be listed in order of preference. The minimum length is 4 octets. The length should always be a multiple of 4.	11
Host Name (String)	Configures the name of the client. The minimum length is 1.	12
Boot file size (String)	Configures the length (in 512-octets blocks) of the default boot image for the client.	13
Merit Dump File (String)	Configures the path name of a file to which the client's core image should be dumped when the client crashes. The minimum length is 1.	14
Domain Name (String)	Configures the domain name that client uses while resolving host names through the domain name system. The minimum length is 1.	15
Swap Server (IP Format)	Configures the IP address of the client's swap server. The length is 4.	16
Root Path (String)	Configures the path name containing the client's root disk. The minimum length is 1.	17
Extensions Path (String)	Configures a file that is retrievable through TFTP. This file contains information that can be interpreted in the same way as the 64-octet vendor-extension field within the BOOTP response, with the following exceptions: The length of the file is unconstrained. All references to Tag 18 (that is, instances of the BOOTP Extensions Path field) within the file are ignored. The minimum length is 1.	18
IP Forwarding Enable/Disable (Integer)	Configures whether the client should configure its IP layer for packet forwarding. Value 0 means disable IP forwarding, and value 1 means enable IP forwarding. The length is 1.	19
Non-local Source Routing Enable/Disable (Integer)	Configures whether the client should configure its IP layer to allow forwarding of datagram with non-local source routes. Value 0 means disable forwarding of such datagram, and value 1 means enable forwarding of such datagram. The length is 1.	20
Policy Filter (IP Format)	Configures policy filters for non-local source routing. The filters consist of a list of IP addresses and masks that specify destination/mask pairs with which to filter incoming source routes. The client should discard any source-routed datagram whose next-hop address does not match with anyone of the	21

Option	Description	Option Code
	filters. The minimum length is 8. The length should always be a multiple of 8.	
Maximum Datagram Reassembly Size (Integer)	Configures the maximum size datagram that the client should be prepared to reassemble. The code for this option is 22, and the length of this option is 2.	22
Default IP Time-to-live (Integer)	Configures the default time-to-live that the client should use on outgoing datagram. The code for this option is 23, and the length of this option is 1.	23
Path MTU Aging Timeout (Integer	Configures the timeout to use when aging the Path MTU values discovered by Path MTU Discovery. The code for this option is 24, and the length of this option is 4.	24
Path MTU Plateau Table (Integer)	Configures a table of MTU sizes to use when performing path MTU discovery. The table is formatted as a list of values, ordered from smallest to largest. The minimum length is 2. The length should always be a multiple of 2.	25
Interface MTU (Integer)	Configures the MTU to be used on the interface. The MTU is specified as a 16-bit unsigned integer. The minimum value is 68.	26
All Subnets are Local (Integer)	Configures whether the client assumes that all subnets of the IP network to which the client is connected use the same MTU as the subnet of that network to which the client is directly connected. Value 1 means that all subnets share the same MTU, and value 0 means that some subnets of the directly connected network have smaller MTUs. The length is 1.	27
Broadcast Address (IP Format)	Configures the broadcast address used on the client's subnet. The length is 4.	28
Perform Mask Discovery (Integer)	Configures whether the client should perform subnet mask discovery using ICMP. Value 0 means that the client should not perform mask discovery, and value 1 means that the client should perform mask discovery. The length is 1.	29
Mask Supplier (Integer)	Configures whether the client should respond to subnet mask requests using ICMP. Value 0 means that the client should not respond, and value 1 means that the client should respond. The length is 1.	30
Perform Router Discovery (Integer)	Configures whether the client should solicit routers using the router discovery mechanism. Value 0 means that the client should not perform router discovery, and value 1 means that the client should perform router discovery. The length is 1.	31

Option	Description	Option Code
Router Solicitation Address (IP Format)	Configures the address to which the client should transmit router solicitation requests. The length is 4.	32
Static Route (IP Format)	Configures a list of static routes that the client should install in its routing cache. The minimum length is 8. The length should always be a multiple of 8.	33
Trailer Encapsulation (Integer)	Configures whether the client should negotiate the use of trailers when using the ARP protocol. Value 0 means that the client should not attempt to use trailers, and value 1 means that the client should attempt to use trailers. The length is 1.	34
ARP Cache Timeout (Integer)	Configures the timeout (in seconds) for ARP cache entries. The time is specified as a 32-bit unsigned integer. The length is 4.	35
Ethernet Encapsulation (Integer)	Configures whether the client should use Ethernet version 2 (RFC 894) or IEEE 802.3 (RFC 1042) encapsulation if the interface is an Ethernet. Value 0 means that the client should use RFC 894 encapsulation, and value 1 means that the client should use RFC 1042 encapsulation. The length is 1.	36
Default TCP TTL (Integer)	Configures the default TTL that the client should use when sending TCP segments. The code for this option is 37, and the length of this option is 1	37
TCP Keepalive Interval (Integer)	Configures the interval that the client TCP should wait before sending a keepalive message on a TCP connection. Value 0 means that the client should not generate keepalive messages on connections unless specifically requested by an application. The code for this option is 38, and the length of this option is 4.	38
TCP keepalive Garbage (Integer)	Configures whether the client should send TCP keep-alive messages with an octet of garbage for compatibility with older implementations. Value 0 means that a garbage octet should not be sent, and value 1 means that a garbage octet should be sent. The length is 1.	39
Network Information Service Domain (String)	Configures the name of the client's NIS domain. The minimum length is 1.	40
Network Information Server (IP Format)	Configures a list of IP addresses indicating NIS servers available to the client. The minimum length is 4. The length should always be a multiple of 4.	41
Network Time Protocol server (IP Format)	Configures a list of IP addresses indicating NTP servers available to the client. The minimum length is 4. The length should always be a multiple of 4.	42

Option	Description	Option Code
Vendor specific information	Allows DHCP server to configure Vendor Specific Information for the corresponding DHCP server address pool. The code for this option is 43 and the minimum length of this option is 1.	43
NetBIOS over TCP/IP name server (IP Format)	Configures a list of RFC 1001/1002 NBNS name servers. The minimum length is 4 octets. The length should always be a multiple of 4.	44
NetBIOS over TCP/IP Datagram Distribution Server (IP Format)	Configures a list of RFC 1001/1002 NBDD servers. The minimum length is 4 octets. The length should always be a multiple of 4.	45
NetBIOS over TCP/IP Node Type (Integer)	Allows NetBIOS over TCP/IP client, which are configured as described in RFC 1001/1002.The length is 1.	46
NetBIOS over TCP/IP Scope (String)	Configures the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002.The minimum length is 1.	47
X Window System Font Server (IP Format)	Configures a list of X window system font servers available to the client. The minimum length is 4 octets. The length should always be a multiple of 4.	48
Window System Display Manager (IP Format)	Configures a list of IP addresses of systems that are running the X window system display manager and are available to the client. The minimum length is 4. The length should always be a multiple of 4.	49
Lease Time (Integer)	Allows the client to request a lease time for the IP address in a client request, and the DHCP server to specify the lease time it is willing to offer in a server reply. The code for this option is 51 and the length of this option is 4.	51
Vendor Class Identifier(String)	The VCI is a text string that uniquely identifies a type of vendor device or info. It is used by DHCP clients in order to “identify itself “to the DHCP server. The code for this option is 60 and the minimum length of this option is 1.	60
NetWare/IP Domain Name	Conveys the NetWare/IP domain name used by the NetWare/IP product. The code for this option is 62, and the maximum length of this option is 255	62
NetWare/IP information	Conveys all NetWare/IP related information except NetWare/IP domain name. The code for this option is 63, and the maximum length of this option is 255.	63
Network Information Service+ Domain (String)	Configures the name of the client's NIS and domain. The minimum length is 1.	64

Option	Description	Option Code
Network Information Service+ Servers (IP Format)	Configures a list of IP addresses indicating NIS and servers available to the client. The minimum length is 4. The length should always be a multiple of 4.	65
TFTP Server Name (IP Format/String)	Allows identifying a TFTP server when the same field in the DHCP header is used for DHCP options. The minimum length is 1.	66
Bootfile Name (String)	Allows identifying a bootfile when the file field in the DHCP header is used for DHCP options. The minimum length is 1.	67
Mobile IP Home Agent (IP Format)	Configures a list of IP addresses indicating mobile IP home Agents available to the client. The minimum length is 0 (indicating no home Agents available). The length should always be a multiple of 4.	68
SMTP Server (IP Format)	Configures a list of SMTP (Simple Mail Transfer Protocol) servers available to the client. The minimum length is 4 octets. The length should always be a multiple of 4.	69
POP3 Server (IP Format)	Configures a list of POP3 servers available to the client. The minimum length is 4 octets. The length should always be a multiple of 4.	70
NNTP Server (IP Format)	Configures a list of NNTP servers available to the client. The minimum length is 4 octets. The length should always be a multiple of 4.	71
Default WWW server (IP Format)	Configures a list of WWW (World Wide Web) servers available to the client. The minimum length is 4 octets. The length should always be a multiple of 4.	72
Finger Server (IP Format)	Configures a list of finger servers available to the client. The minimum length is 4 octets. The length should always be a multiple of 4.	73
Default Internet Relay Chat Server (IP Format)	Configures a list of IRC servers available to the client. The minimum length is 4 octets. The length should always be a multiple of 4.	74
Street Talk Server (IP Format)	Configures a list of Street Talk servers available to the client. The minimum length is 4 octets. The length should always be a multiple of 4.	75

Option	Description	Option Code
Street Talk Directory Assistance Server (IP Format)	Configures a list of STDA servers available to the client. The minimum length is 4 octets. The length should always be a multiple of 4.	76
User Class Information	Configures the user class of which the client is a member. The code for this option is 77.	77
SLP Directory Agent (IP Format)	Configures a list of IP addresses for Directory Agents. The code for this option is 78.	78
SLP Service Scope (IP Format)	Configures a list of scopes that a SLP Agent is configured to use. The code for this option is 79.	79
Rapid Commit (Integer	Indicates the use of the two-message exchange for address assignment. The code for this option is 80.	80
Internet Storage Name Service (IP Format)	Configures the location of the primary and backup iSNS servers and the iSNS services available to an iSNS client. The code for this option is 83.	83
Relay Agent Information	This option is a "container" option for specific Agent-supplied sub-options. Allows the DHCP relay to specify flags for the forwarded packet. The code for this option is 84.	84
NDS Servers (IP Format)	Configures NDS servers for the client to contact for access to the NDS database. The code for this option is 85. The minimum length of this option is 4 octets, and the length must be a multiple of 4.	85
NDS Tree Name (String)	Configures the name of the NDS tree that the client will be contacting. The code for this option is 86, and the maximum length of this option is 255 bytes.	86
NDS Context (String)	Configures the initial NDS context that the client should use. This option can appear more than once in the DHCP packet. The code for this option is 87. The maximum length for each instance of this option is 255, but, as just described, the option may appear more than once if the desired NDS context takes up more than 255 octets.	87
BCMCS Controller Domain Name List (String)	Configures a list of domain names of the BCMCS controller.	88
BCMCS Controller IPv4 address List (IP Format)	Configures a list of IPv4 addresses of the BCMCS controllers. The code for this option is 89. The minimum length of this option is 4, and the length must be a multiple of 4.	89

Option	Description	Option Code
Authentication	Configures the DHCP authorization details through which authorization tickets can be generated.	90
Client-Last-Transaction-Time (Integer)	Allows the receiver to determine the time of the most recent access of the client. The code for this option is 91, and the length of this option is 4 octets	91
Client System Architecture Type (Integer)	Configures a list of architecture types supported by the client. The code for this option is 93.	93
LDAP, Lightweight Directory Access Protocol	Allows the client to receive an LDAP URL of the closest available LDAP server/replica that can be used to authenticate users or look up any useful data. The code for this option is 95.	95
Client Machine Identifier (Integer)	Configures the 16 octet Globally Unique Identifier of the PXE compliant clients. This option must be present in all DHCP and PXE packets sent by PXE-compliant clients and servers. The code for this option is 97.	97
Open Group's User Authentication (String)	Configures a list of URLs, each pointing to a user authentication service that is capable of processing authentication requests encapsulated in the UAP (User Authentication Protocol). The code for this option is 98. Length of this option is the length of the URL list in octets. URL list contains one or more URLs separated by ASCII space character	98
GEOCONF_CIVIC	DHCPv4 servers should return GEOCONF_CIVIC option only when the DHCPv4 client has included this option in its 'parameter request list'. The code for this option is 99. The minimum length is 3 octets	99
Printer Name (String)	Configures names of the printers available for the client.	100
NetInfo Parent Server (IP Format)	Allows the clients to obtain the address of the parent server for their local NetInfo domain. The length of this option is 4. The minimum length of this option is 1.	112
NetInfo Parent Server Tag (Integer)	Allows the clients to obtain the tag of the NetInfo parent server, if the tag is different from the default value "network". The minimum length of this option is 1.	113
Auto-Configure (Integer)	Configures whether auto-configuration should be disabled on the local subnet. Value 0 means do not auto-configure, and value 1 means auto-configure.	116

Option	Description	Option Code
Name Service Search (Integer)	Configures the order in which name services should be consulted when resolving hostnames and other information. The minimum length of this option is 2 octets.	117
Subnet - Selection (IP Format)	Configures a single IPv4 address, which is the address of a subnet.	118
DNS Domain Search List (String)	Configures the domain search list that is used when resolving hostnames using DNS.	119
SIP Server (IP Format or Domain Name)	Configures a maximum of either two IPv4 addresses or Domain Names that can be mapped to SIP (Session initiation Protocol) outbound proxy servers. This is one of the methods that a SIP client uses to obtain the addresses of a local SIP server.	120
Classless Static Route (IP Format)	Configures a list of static routes, each containing a destination descriptor and the IP address of the router that should be used to reach that destination.	121
CCC, CableLabs Client Configuration	Allows to configure various devices deployed within CableLabs architecture.	122
GeoConf	Configures the LCI (Location configuration information) of the client. The information includes latitude, longitude, and altitude.	123
Vendor-Identifying Vendor Class	Allows DHCP client to unambiguously identify the vendor that manufactured the hardware on which the client is running, the software in use, or an industry consortium to which the vendor belongs.	124
Vendor-Identifying Vendor-Specific	DHCP clients and servers use this option to exchange vendor-specific information.	125
IP Telephone Configuration Assignment (string)	Specifies that the IP phone should be setup using dynamic IP and time should be synchronized with a time server.	128
WLAN IP Telephony Manager (IP Format)	Configures the wireless IP telephony that allows converged voice and data traffic over a common wireless network so as to simplify network infrastructure.	151
IP Telephone VLAN Identifier (String)	Configures the IP telephone VLAN ID that is used to automatically determine voice VLAN using DHCP.	191
Option 240 (String)	Configures the dhcp option type to request the server to get the Option 240 information. The minimum length returned by the server is 1.	240

Option	Description	Option Code
Enter Option Code Manually	Allows the user to manually configure the DHCP option and its corresponding code and value.	User enters Option code

Chapter 25

IGMP Snooping

IGMP (Internet Group Management Protocol) is the protocol, a host uses to inform a router when it joins (or leaves) an Internet multicast group. IGMP is only used on a local network; a router must use another multicast routing protocol to inform other routers of group membership. IGS (IGMP Snooping) is a feature that allows the switch to listen in on the IGMP conversation between hosts and routers.

In IGS, a host computer uses IGMP to inform a router that it intends to listen to a specific multicast address. If another computer snoops such packets, the other computer can learn the multicast sessions to which the computers on the local network are listening.

IGS significantly reduces traffic from streaming media and other bandwidth-intensive IP multicast applications.

To access IGMP Snooping screens, click **Multicast > IGMP Snooping**

IGMP Snooping related parameters are configured through the screens displayed by the following tabs:

- Basic Settings
- Timer
- Vlan Configuration
- Interface Configuration
- Router Port Conf
- Router Ports
- Static Entry
- Fwd Information
- Mcast Receiver Info

By default, the tab **Basic Settings** displays the **IGMP Snooping Configuration** is displayed.

26.1 IGMP Snooping Configuration

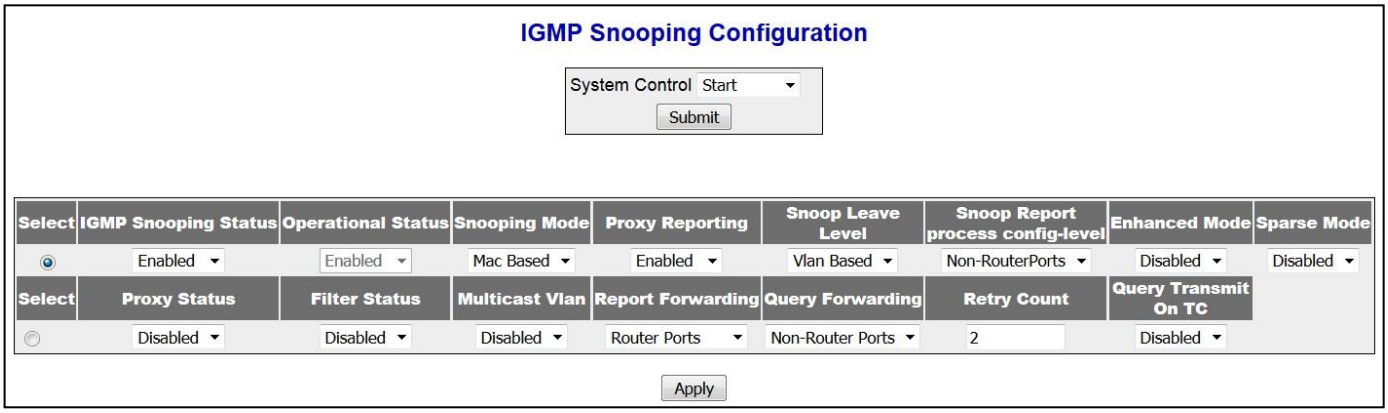


Figure 26-1 : IGMP Snooping Configuration

Screen Objective	This screen allows the user to configure basic settings such as IGMP snooping status, operational status, Snooping Mode, Proxy Reporting and Snoop Leave level.
☞	• The fields in second row of the form at the bottom can be modified by clicking on the select option in the second row.
Navigation	**Multicast > IGMP Snooping > Basic Settings**
Fields	• **Select** - Select the option button to configure the selected parameters • **System Control** - Select the System Control status of IGS in the switch.The default option is **Start**. The list contains: – **Start** – Starts the IGMP snooping protocol and allocates the resources required by the IGS module. During protocol start-up, it creates semaphore, RBTree, hash table and also initializes the timer task. – **Shutdown** - All the resources are released back to the system and the module stops running. All the timers are stopped. The RBTree and hash Table and the allocated memory pools are deleted. • **IGMP Snooping Status** - Select the Global status of IGS in the switch.The default option is **Disabled**. The list contains: – **Enabled** – Starts the IGMP snooping protocol operations. – **Disabled** – Stops performing the IGMP snooping protocol operations. • **Operational Status** - Displays the Operational status of the IGS in the switch. The default option is **disabled**. The list contains: – **Enabled** – Indicates that IGS protocol is currently enabled in the system. – **Disabled** - Indicates that IGS protocol is currently disabled in the system.

- **Snooping Mode** - Select the IGMP snooping mode. Modes are provided with redundancy support. The default option is **MAC Based**. The list contains:
  - **IP based** – IGS protocol operation is based on the IP address and group address. This mode is chosen if the hardware supports programming of S, G and *, and G entries
  - **MAC based** - Hardware supports only MAC based multicast tables and the snooping protocol operation is based only on the group address.
- **Proxy Reporting** - Select the Proxy Reporting status in the switch. IGS network traffic gets reduced. The default option is **Enabled**. The list contains:
  - **Enabled** - Switch generates reports and forwards them to the router, based on the available host information.
  - **Disabled** – Switch acts as transparent snooping bridge. The switch forwards all v3 reports and a single v2 report to the router.
- **Snoop Leave Level** - Select the leave processing mechanism to be implemented at the VLAN level or at port level. When the switch intercepts a leave group message on a switch port, it normally sends a query to that multicast group through the same switch port. If no hosts respond to the query and no multicast routers have been discovered on the switch port, that port is removed from the multicast group. The default option is **Vlan Based**. The list contains:
  - **Vlan Based** – Configures the leave mechanism at the VLAN level. In Vlan based leave processing mode, the fast leave functionality configurable per VLAN or normal leave configurations are available for processing leave messages.
  - **Port Based** – Configures the leave mechanism at port level. In port based leave processing mode, the explicit host tracking functionality, the fast leave functionality or normal leave configurable on an interface can be used for processing the leave messages.
- **Snoop report Process Config Level** - Select the report processing mechanism to be used for handling the incoming report messages to be processed. The default option is **Non-RouterPorts**. The list contains:
  - **Non-RouterPorts** – The incoming report messages are processed only in the non-router ports. Report message received on the router ports are not processed.
  - **All-Ports** – The incoming report messages are processed in all the ports inclusive of router ports.
- **Enhanced Mode** - Select the operating status of snooping module. The default option is **Disabled**. The list contains:
  - **Enabled** – The snooping module operates in enhanced mode. It is a mode of operation provided to enhance the operation of IGMP snooping module to duplicate Multicast traffic by learning Multicast group entries based on the Port and Inner Vlan. This mode of operation is applied when the downstream devices are less intelligent or not capable of duplicating Multicast traffic. The module multicasts from an Outer VLAN (SVLAN) to a set of ports & Inner VLANs (CVLAN). In this mode, an S-

tagged multicast data or query packet from one port can result in multiple copies of the packet on the same egress port, each with a different C-tag. The Inner VLAN (CVLAN) will typically have a valid value within the designated range.

- **Disabled** – The snooping module operates in default mode. This mode of operation is applied when downstream device is capable of performing duplication of Multicast traffic. In the this mode, the module multicasts from an Outer VLAN (SVLAN) to a set of ports. The Inner VLAN (CVLAN) will typically have a value of zero. In this mode, an S-tagged multicast data or query packet from one port can result in multiple packets on separate egress ports, but only one packet on any one egress port with an S-tag or with no tag.

Enhanced mode is in enabled state only when the snooping mode is set as IP Based

- **Sparse Mode** - Select whether the snooping module operates in the sparse mode or non-sparse mode. This option is to select whether the unknown multicast traffic should be dropped or flooded when there is no interested listener. The default option is **disabled**. The list contains:
  - **Enabled** – The IGS module drops the unknown multicast traffic when there is no listener for the multicast data
  - **Disabled** – The IGS module forwards the unknown multicast traffic. The multicast data gets flooded to the member port of VLAN.

Sparse mode is in enabled state, only when the snooping mode is set as IP Based.

- **Proxy Status** - Select the status of the Proxy in the system. In proxy mode all the reports and queries generated by the switch will be having the switch IP as the source IP. The list contains:
  - **Enabled** – Enables proxy in the system. The switch act as querier for all downstream interfaces and act as host for all upstream interfaces.
  - **Disabled** – Disables proxy in the system.

Proxy status can be enabled only if Proxy-reporting is disabled

- **Filter Status** - Select the filter status. The default option is **Disabled**. The list contains:
  - **Enabled** – Enables the IGS filtering feature. The channel registration is restricted from addition to the database if it is to be filtered. In transparent snooping, the filtered packet will not be added to the snooping database but will be forwarded upstream.
  - **Disabled** – Disables the IGS filtering feature. All filter related configurations are allowed but the incoming report will not be subjected to the filter process. IGS module programs the hardware to remove the configured rate limit. It flushes all the registrations learnt through a port if a threshold limit is configured for this interface.

- **Multicast Vlan** - Select the multicast VLAN status. Multicast VLAN feature can be used for applications where wide-scale deployment of multicast traffic is necessary. MVLAN registration allows a subscriber on a port to subscribe and unsubscribe to a particular multicast stream on any of the

multicast VLANs. Multicast VLANs enable efficient multicast data flow in separate M-VLANs, while normal data flows through other/different VLANs. The default option is **Disabled**. The list contains:

- **Enabled** – Enables the multicast Vlan feature. Router sends a single copy of the data for the particular MVLAN, instead of forwarding a separate copy of the multicast data to each VLAN. This saves the network bandwidth.
- **Disabled** – Disables the multicast Vlan feature. A separate copy of the multicast data has to be forwarded from the router in the absence of M-VLAN.

- **Report Forwarding** - Select whether the report must be forwarded on all ports or only on router ports. The port which receives the query message from the router is the Router port. The default option is **Router Ports**. The list contains:
  - **Router Ports** – Forwards reports only on the router ports
  - **All Ports** – Forwards reports on all ports of the VLAN
  - **Non-edge** - Forwards the reports on non-edge ports detected by spanning tree protocol

- **Query Forwarding** - Select whether the query to be forwarded to the entire member ports of the VLAN or to Non-router Ports. The default option is **Non-Router Ports**. The list contains:
  - **All Ports** – The query messages are forwarded to all the member ports of the VLAN.
  - **Non-Router Ports** – The query messages are forwarded only to the non-router ports.

- **Retry Count** - Enter the maximum number of group specific queries sent on a port on reception of an IGMPv2 leave message. This values ranges between 1 and 5. The default value is **2**.

  When the switch receives leave message on a port, it sends group specific query to check if there are any other interested receivers for the group. The Retry Count defines the maximum number of queries sent by the switch before deleting the port from the group membership information in the forwarding database. If the maximum retry count exceeds the RetryCount, then the port will be deleted from the multicast group membership information in the forwarding database and received leave message will be forwarded onto the router ports if there are no interested receivers for the group.

- **Query Transmit on TC** - Select path redundancy for IGMP Snooping queries transmission to be enabled or disabled whenever topology changes. The default option is **Disabled**. The list contains:
  - **Enabled** - Provides path redundancy while preventing undesirable loops in the network. When enabled allows the path to exchange information so that only one of them will handle a given message that is being sent between two computers within the network.
  - **Disabled** - Path redundancy is disabled and it leads to flooding of data.

Buttons	• **Submit** - To modify attributes and save the changes. • **Apply** - To modify attributes for the selected entry and save the changes.

26.2 IGMP Snooping Timer Settings

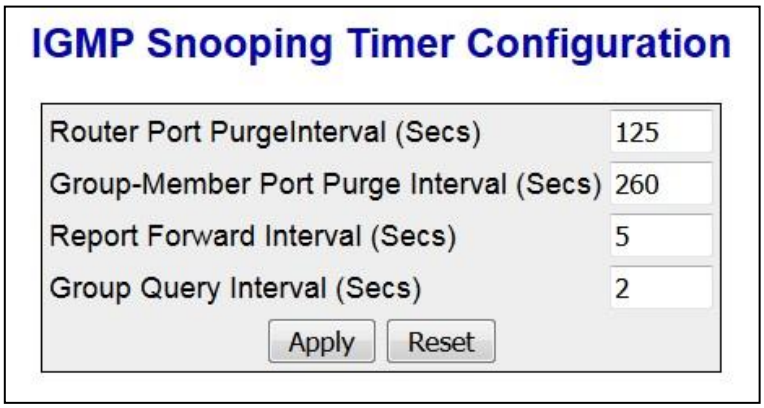


Figure 26-2 : IGMP Snooping Timer Settings

Screen Objective	This screen allows the user to set Router port purge interval, Group-Member Port Purge Interval, Report Forward Interval and Group Query Interval.
Navigation	**Multicast > IGMP Snooping > Timer**
Fields	• **Router Port Purge Interval (Secs)** - Enter the time interval after which the learnt router port will be purged. This option is to determine the aliveness of router ports. This value ranges from 60 to 600 seconds. The default value is **125** seconds. For each router port learnt, the timer runs for the configured port purge time interval. When the timer expires, the learnt router port entry is purged. If control messages are received from the router before the timer expiry, then the timer is restarted. • **Group-Member Port Purge Interval (Secs)** - Enter the time interval after which a learnt port entry is purged, if IGMP reports are not received on a port. This value ranges from 130 to 1225 seconds. The default value is **260** seconds. For each port on which report has been received, this timer runs for the configured time. This timer will be restarted whenever a report message is received from a host on the specific port. If the timer expires, then, the learnt port entry will be purged from the multicast group. • **Report Forward Interval (Secs)** - Enter the time interval within which the next report messages for the same multicast group will not be forwarded. This timer is used when both proxy and proxy-reporting is

disabled. This option is to perform Join Aggregation of IGMP membership report. This value ranges from 1 to 25 seconds. The default value is **5** seconds.

> This is the interval (in seconds) within which report messages for the same multicast group will not be forwarded. The Report Forward Timer is per multicast group. This timer is started as soon as a report message for that group is forwarded out. Within this **ReportForwardInterval** if another report for the same group arrives, then that report will not be forwarded

- **Group Query Interval (Secs)** - Enter the interval value in which the snooping switch waits for the membership reports from the interested receivers for the given multicast group after sending out query messages. This value ranges from 2 to 5 seconds. The default value is **2** seconds.

Buttons

- **Apply** - To modify attributes and save the changes.
- **Reset** - To reset to default value for respective fields and discard all user inputs.

26.3 IGMP Snooping VLAN Configuration

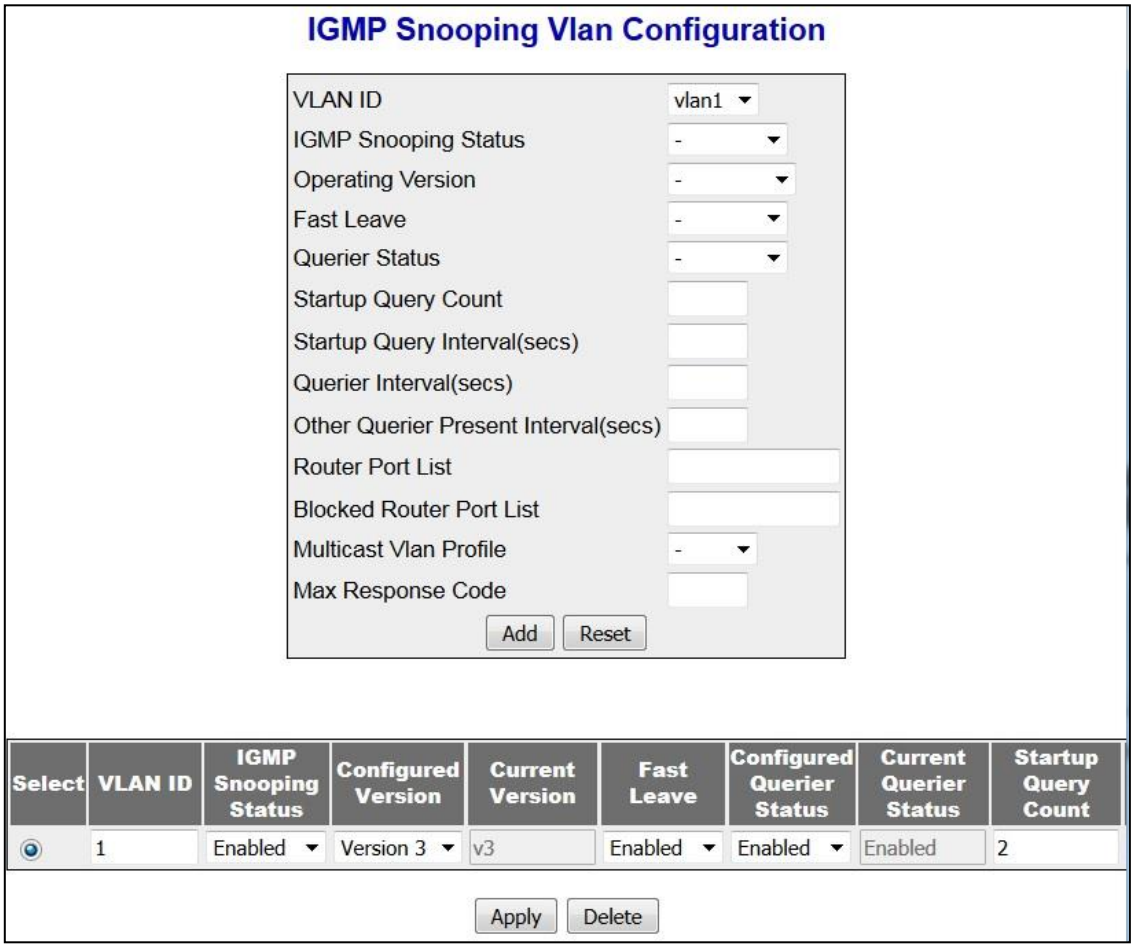


Figure 26-3 : IGMP Snooping Vlan Configuration Part A

Startup Query Interval(secs)	Querier Interval(secs)	Other Querier Present Interval(secs)	Router Port List	Blocked Router Port List	Multicast Vlan Profile	Max Response Code
31	125	255	NONE	NONE	0	100

Figure 26-4 : IGMP Snooping Vlan Configuration Part B

Screen Objective	This screen allows the user to configure IGMP Snooping on specific VLANs
Navigation	**Multicast > IGMP Snooping > VlanConfiguration**
Fields	• **VLAN ID** - Select the VLAN Identifier that uniquely identifies a specific VLAN from the list specified already in the system. The IGMP snooping configuration is performed for this specific VLAN ID.

- **IGMP Snooping Status** - Select the status of IGMP snooping on the specified VLAN. The default option is **Disabled**. The list contains:
  - **Enabled** – IGS is enabled on the specified VLAN. A switch will listen for IGMP messages from the host connected on those interfaces and build the software. This ensures that only the ports that require a given multicast stream actually receive it.
  - **Disabled** - IGS is disabled on the specified VLAN.
- **Operating Version/ Configured Version** - Select the Operating Version of IGS for the specified VLAN. The default option is **Version 3**. The list contains:
  - **Version 1** – The port list connected to listeners of Multicast groups is built based on IGMP membership Reports, Query and Leave messages
  - **Version 2** – The port list connected to listeners of Multicast groups is built based on IGMP membership Reports, Query and Leave messages, added support for low leave latency, that is, a reduction in the time it takes for a multicast router to learn that there are no longer any member of a particular group present on an attached network.
  - **Version 3** - The port list is based on source filtering information sent by IGMPv3 hosts in their membership reports to build Source specific Multicast groups. Support for source filtering, that is, the ability for a system to report interest in receiving packets only from specific source addresses, or from other than specific source addresses, sent to a particular multicast address.
- **Fast Leave** - Select the Fast Leave status of IGS. The default option is **Disabled**. The list contains:
  - **Enabled** - On receipt of a single leave message, the port information is immediately removed from the multicast group entry. The switch immediately removes the port from the forwarding table without sending a group specific query. The fast leave functionality does not verify if other interested receivers are still present for the multicast group on the same port.
  - **Disabled** - Normal leave functionality gets enabled. The switch checks if there are any interested receivers for the group by sending a group specific query before removing the port from the forwarding table.
- **Querier Status/ Configured Querier Status** - Select whether the switch is configured as a querier in a VLAN. The default option is **Disabled**. The list contains:
  - **Enabled** – The switch starts acting as a querier and sends query messages until it receives best querier information. The switch sends general queries at regular time intervals. This querier message takes part in querier election.
  - **Disabled** – The switch is configured as non-querier, does not propagate any general query messages and does not take part in querier election.
- **Startup Query Count** - Enter the number of queries to be sent during startup of querier election process at the interval of startup query interval. This value ranges from 2 to 5. The default value is **2**.

- **Startup Query Interval(secs)** - Enter the interval (in seconds) between the startup general query messages sent by the switch (querier) during the startup of querier election process. This value ranges from 15 to 150 seconds. The default value is **32** seconds.

  This value should be less than or equal to one fourth of query interval value configured for the VLAN.

- **Querier Interval (secs)** - Enter the time period between which the general queries are sent by IGMP snooping, when the switch is configured as querier on a VLAN. The switch waits for the configured time period after sending a general query message. On the expiry of this query interval, the switch again sends the general query message and restarts the timer. This value range between 6 and 600 seconds. The default value is **125** seconds.

- **Other Querier Present Interval(secs)** - Enter the time period (in seconds) that must pass before a multicast router decides that there is no longer another multicast router which should be the querier. This value ranges from 120 to 1215 seconds. The default value is **255** seconds.

  This value must be >= ((Robustness Variable * Query Interval) + (Query Response Interval/2)).

  The Robustness Variable tunes IGMP to expected losses on a link. IGMPv3 is robust to (Robustness Variable - 1) packet losses.

- **Router Port List** - Enter the static Router port list for VLAN. When the snooping switch receives a Router advertisement message through a port, the port is identified as router port and is added in the router port list. The default option is **None**.

- **Blocked Router Port List** - Enter the list of ports which are configured statically as blocked router ports. On a blocked router port the software discards queries, PIM/DVMRP and Data Messages and prevents the port from ever becoming a router port. The blocked router port feature does not involve any hardware programming. Multicast data is dropped on a blocked router port. Reports are not forwarded to a blocked router port. Reports coming from blocked router port are not processed. The default option is **None**.

  A port cannot be configured as blocked router port, if it is already configured as static router port

- **Multicast Vlan Profile** - Select the multicast profile identification configured for a particular VLAN and is used for multicast VLAN classification. When any untagged report or leave message is received and the Group & Source address in the received packet matches any rule in this profile, the received packet is classified to be associated with the VLAN to which this profile is mapped.

- **Max Response Code** - Enter the maximum response code advertised in queries which are sent over this VLAN. This value ranges from 0 to 255 tenths of a second. The default value is 10**0**.

	• **Current Version** - Displays the working IGMP Version on the given VLAN. The value can be version 1, version 2 or version 3. • **Current Querier Status** - Displays the current querier status in the VLAN. The value can be enabled or disabled.
Buttons	• **Add** - To add and save new configuration. • **Reset** - To reset to default value for respective fields and discard all user inputs. • **Apply** - To modify attributes for the selected entry and save the changes. • **Delete** - To delete the selected entry.

26.4 IGMP Snooping Interface Configuration

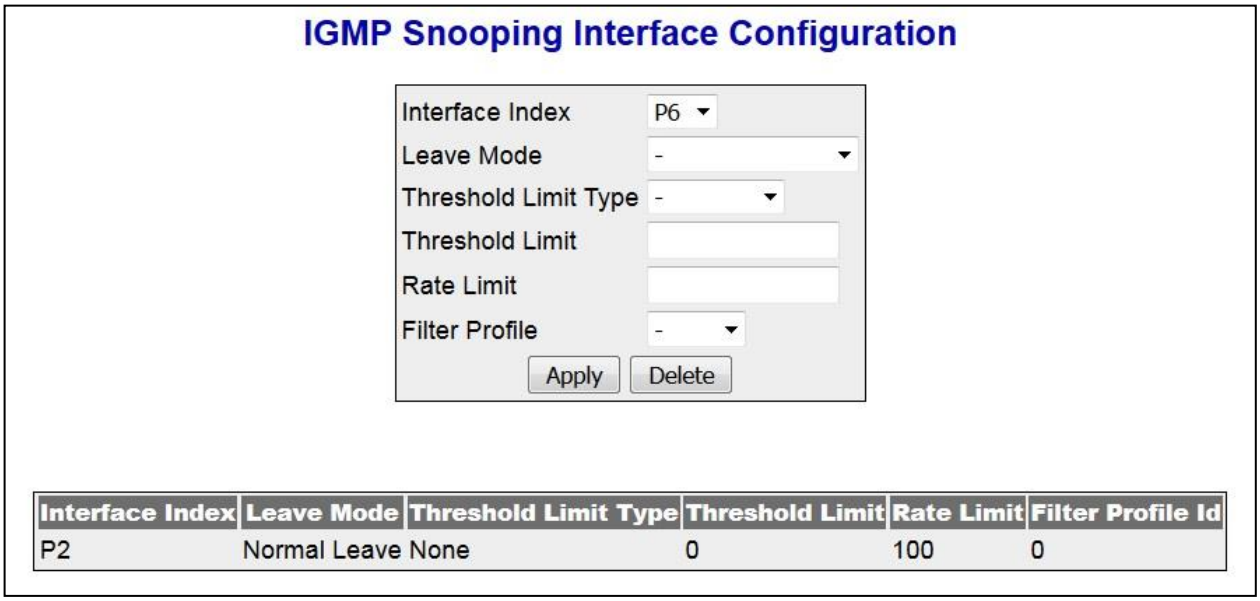


Figure 26-5 : IGMP Snooping Interface Configuration

Screen Objective	This screen allows the user to configure IGMP Snooping on specific interface.
Navigation	**Multicast > IGMP Snooping > InterfaceConfiguration**
Fields	• **Interface Index** - Select the interface index of the port from the list specified already in the system. • **Leave Mode** - Select the mechanism to be used for processing leave messages in the down stream interface. The default option is **Normal Leave.** The list contains:

- **Explicit Tracking** – Leave messages are processed using the explicit tracking mechanism. On receipt of the leave message, the switch uses its learnt database to determine whether the specified multicast group has a single receiver or multiple receivers attached to the port. The switch removes the port from the multicast group entry only when no other receivers are present in the same group.
- **Fast Leave** – Leave messages are processed using the fast leave mechanism. On receipt of a single leave message the port is immediately removed from the group entry. The fast leave functionality does not verify if other interested receivers are still present in the multicast group on the same port. Hence the feature can be used effectively only in a point-to-point connection
- **Normal Leave** – A group or group specific query is sent on the interface when a leave message is received. Once snooping switch sends the leave message for a multicast group, the snooping switch sends out query messages and waits for a specified time for the membership reports from the interested receivers for the given multicast group.


This field can be configured only when the Snoop Leave Level is set to Port Based.

- **Threshold Limit Type** - Select the type of limit to be applied for the interface. The threshold limit will be applied when reports are received from the downstream interface. The default option is **None**. The list contains:
  - **None** – No limiting is done.
  - **Groups** – Limits the IGMP report message based on the group registration allowed per downstream interface.
  - **Channels** – Limit is applied only for IGMPv3 Include and Allow reports based on the S, G registration that are allowed per downstream interface.


The channel limit is applied only for IGMPv3 include and allow reports. The group limit is applied for all IGMP reports.

- **Threshold Limit** - Enter the maximum number of unique entries (channel or group) which can be learned simultaneously on the interface. The software allows the configuration of threshold limit per downstream interface. Downstream interface refers to a physical port in the default mode of operation or to a combination of inner VLAN and physical port in the enhanced mode of operation of the switch. This value ranges from 0 to 4294967295. The default value is **0.**


This field can be configured only when the Threshold Limit Type is set.

- **Rate Limit** - Enter the rate limit for a down stream interface in the units of the number of IGMP packets per second. The software calls an NPAPI to configure this limit into the data path/hardware. The MDL rate limit per port will eliminate bursts or attacks coming from the specific physical port and thereby eliminates the case of exhausting the system resources. This value ranges from 0 to 4294967295. The default value is **4294967295**.
- **Filter Profile Id** - Select the Filter Profile Identifier. A unique identifier configured by the administrator for a particular Internet address type

	identifies each of the profile entries. The profile ID is configured for the downstream interface. The default value is **0.**
Buttons	• **Apply** - To modify attributes and save the changes. • **Delete** - To delete the selected entry.

26.5 IGMP Snooping VLAN Router Port Configuration

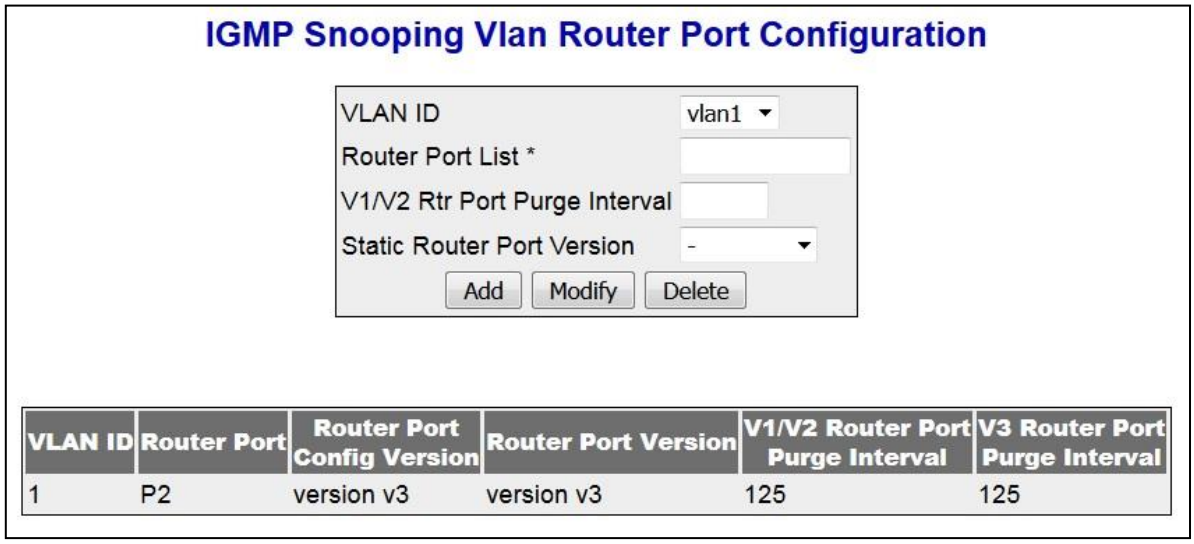


Figure 26-6 : IGMP Snooping Vlan Router Port Configuration

Screen Objective	This screen allows the user to configure the details of the router port.
Navigation	**Multicast > IGMP Snooping > RouterPortConf**
Fields	• **VLAN ID** - Select the VLAN Identifier that uniquely identifies a specific VLAN from the list already specified in the system. The IGMP snooping configuration is performed for the entered VLAN ID. • **Router Port List** - Enter the router port / port list for the VLAN specified in VLAN ID field. When the snooping switch receives a router advertisement message through a port, the port is learnt as router port. These ports are part of this router port list. User can enter the router port / port-list on which he wants to configure the purge interval / version. • **V1/V2 Rtr Port Purge Interval** - Enter the time interval after which the switch assumes that there are no v1/v2 routers present on the upstream port. For each router port learnt, this timer runs for 'RouterPortPurgeInterval' seconds. When the timer expires, the learnt router port entry is purged. If control messages are received from the router before the timer expiry, then the timer is restarted. This value ranges from 60 to 600. The default value is **125**

- **Static Router Port Version** - Select the operating version of the IGMP proxy on the upstream router port from the list already specified in the system. The default option is **Version 3**. The list contains:
  - **Version1** - Indicates that the operating version of IGMP proxy is version1
  - **Version2** - Indicates that the operating version of IGMP proxy is version2
  - **Version3** - Indicates that the operating version of IGMP proxy is version3
- **Router Port** - Displays the interface index of the port which is defined as an upstream router port. When the snooping switch receives a Router advertisement message through a port, the port is identified as router port.
- **Router Port Config Version** - Displays the configured version of the IGMP Proxy on the upstream router port. The default value is **Version 3**
- **Router Port Version** - Displays the operating version of the IGMP proxy on the upstream router port. The default value is **Version 3.**
- **V3 Router Port Purge Interval** - Displays the time interval after which the switch assumes that there are no IGMP v3 routers present on the upstream port. When the timer expires, the learnt router port entry is purged. If control messages are received from the router before the timer expiry, then the timer is restarted. This value ranges from 60 to 600. The default value is **125**.

  For each V3 router port learnt, the timer runs for time interval calculated based on the formula “V3 Router port purge Interval = ((V3 Querier Query Interval * Robustness variable) + Max ResponseTime) seconds

Buttons

- **Add** - To add and save new configuration.
- **Modify** - To modify attributes and save the changes.
- **Delete** - To delete the selected entry.

26.6 IGMP Snooping VLAN Router Ports

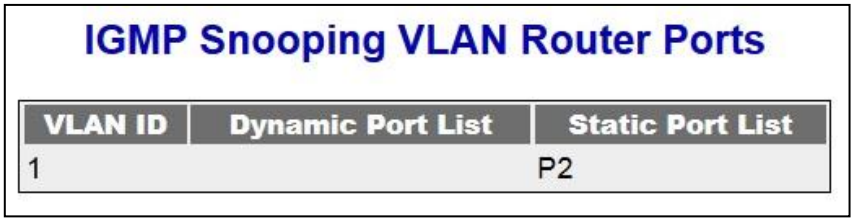


Figure 26-7 : IGMP Snooping VLAN Router Ports

Screen Objective	This screen displays the Router Port List table. The dynamic and static ports are listed in the screen.
Navigation	**Multicast > IGMP Snooping > RouterPorts**
Fields	• **VLAN ID** - Displays the VLAN Identifier that uniquely identifies a specific VLAN on which router ports are learnt / configured. • **Dynamic Port List** - Displays the lists of ports on which routers are present. These router ports are learnt through control messages received from routers and can also be configured statically. • **Static Port List** - Displays the list of ports which are configured statically as router ports. Only static router ports will be restored during save restore. The default operating version for static router ports will be IGMPv3, based on the address type.

26.7 IGMP Snooping Static Configuration

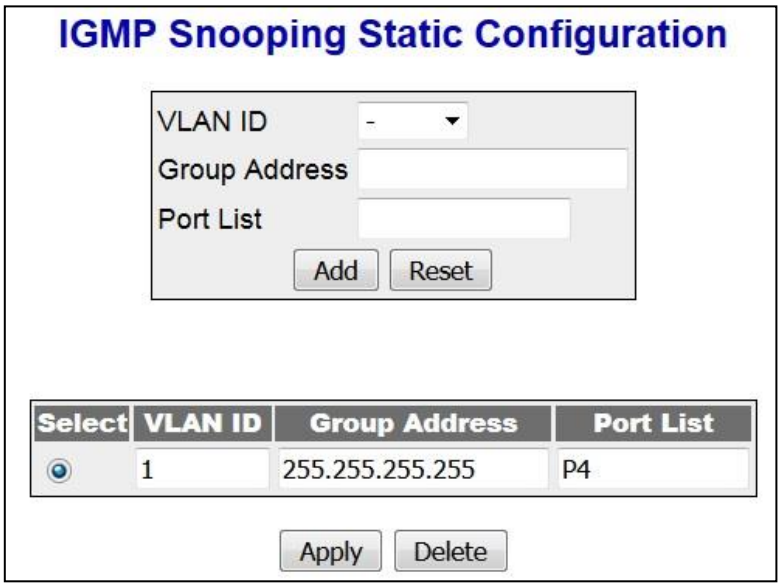


Figure 26-8 : IGMP Snooping Static Configuration - Multicast Group

Screen Objective	This screen allows the user to configure the IGMP snooping on static interface.
Navigation	**Multicast > IGMP Snooping > StaticEntry**

Fields	• **VLAN ID** - Select the VLAN Identifier that uniquely identifies a specific VLAN from the list specified already in the system. The MAC based multicast forwarding entry is displayed for the requested VLAN ID. • **Group Address** - Enter the Group MAC Multicast address that is learnt. • **Port List** - Enter the learnt ports list for which the multicast data packets for the group will be forwarded.
Buttons	• **Add** - To add and save new configuration. • **Reset** - To reset to default value for respective fields and discard all user inputs. • **Apply** - To modify attributes for the selected entry and save the changes. • **Delete** - To delete the selected entry.

26.8 IGMP Snooping MAC / IP Based Multicast Forwarding Table

MAC Based Multicast Forwarding Table

VLAN ID	Group MAC Address	Port List
1	01:00:5e:7f:ff:ff	P2,P4

Figure 26-9 : IGMP Snooping MAC Based Multicast Forwarding Table

IP Based Multicast Forwarding Table

VLAN ID	Source IP Address	Group IP Address	Port List
1	0.0.0.0	225.0.0.1	P1-P2

Figure 26-10 : IGMP Snooping IP Based Multicast Forwarding Table

Screen Objective	This screen displays the IGMP group information such as MAC based or IP based Multicast Forwarding Table and Multicast Forwarding table is populated with list of ports interested in receiving multicast traffic to avoid flooding of multicast data traffic.

☞	When snooping is disabled on the port, all the entries in the group table and forwarding table are deleted for the port.
Navigation	**Multicast > IGMP Snooping > FwdInformation**
Fields	**MAC Based Multicast Forwarding Table** • **VLAN ID** - Displays the VLAN Identifier that uniquely identifies a specific VLAN. The MAC based multicast forwarding entry is displayed for the requested VLAN ID. • **Group MAC Address** - Displays the Group MAC Multicast address that is learnt. • **Port List** - Displays the learnt ports list for which the multicast data packets for the group will be forwarded **IP Based Multicast Forwarding Table** • **VLAN ID** - Displays the VLAN Identifier that uniquely identifies a specific VLAN. The IP based multicast forwarding entry is displayed for the entered VLAN ID. • **Source IP Address** - Displays the unicast source IP address of the data source that sends multicast data to the group. • **Group IP Address** - Displays the IP address of the group that is registered for receiving the multicast traffic. • **Port List** - Displays the learnt ports list for which the multicast data packets for group should be forwarded.

Chapter 26

TAC

TAC (Transmission and Admission Control) is a utility module that can be used by multicast protocols for filtering multicast packets and multicast VLAN classification.

TAC module creates and maintains a set of Group addresses and/or Source addresses in a profile. These profiles are used for purposes of filtering. Profiles in this TAC module can also be used for M-VLAN Classification. The profile table and filter table present in the TAC module are built through administrator configuration. All configured addresses are stored as address ranges. When a report is received on a particular interface, the corresponding profile mapped to this interface is obtained and filter rule table is scanned to determine if a match exists for the address present in the incoming report. If the address is present in the profile with permission as permit, the reports are processed else they are dropped

To access **TAC** screens, click **Multicast > TAC**.

TAC related parameters are configured through the screens displayed in the following tabs

- Profile
- Profile filters

By default, the tab **Profile** displays the **TAC Profile Configuration** screen.

27.1 TAC Profile Configuration

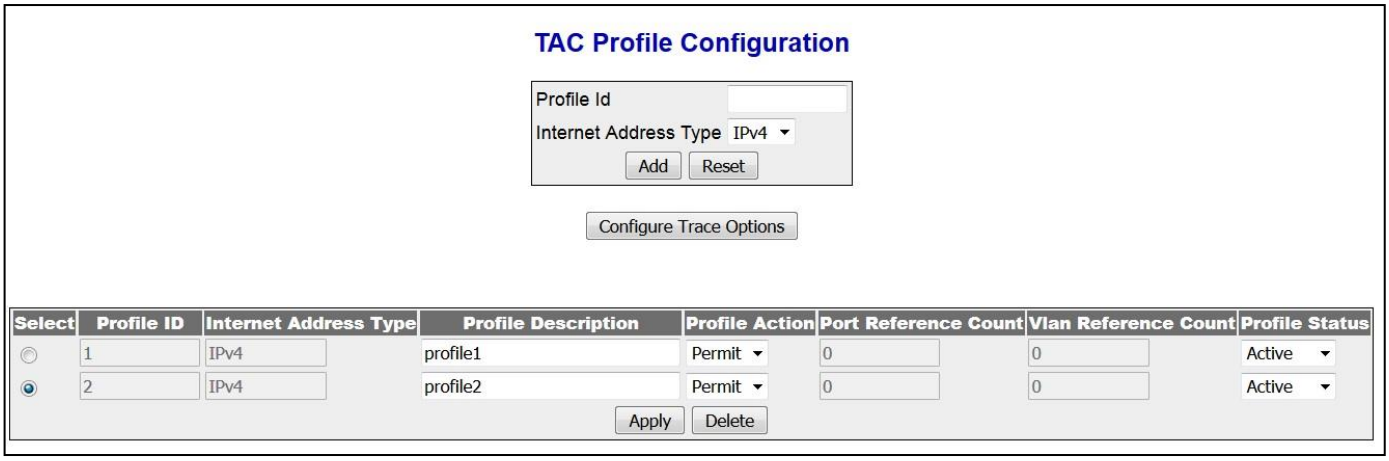


Figure 27-1 : TAC Profile Configuration

Screen Objective	This screen allows the user to configure the multicast profile used to filter incoming IGMP/MLD reports from customers. Each profile table entry contains a table of multicast information and an access rule to permit or deny.
Navigation	**Multicast** > **TAC** > **Profile**
Fields	• **Select** - Click to select the Profile ID for which the configurations need to be modified or deleted. • **Profile Id / Profile ID** - Enter the unique identifier for a multicast profile entry.This value ranges from 1 to 4294967295. • **Internet Address Type** - Select the internet address type in the multicast profile. The list contains: – **IPv4** - Sets the internet address type as IPv4. – **IPv6** - Sets the internet address type as IPv6. • **Profile Description** - Enter the description for the profile entry. This value is a string of maximum size 128. Only characters and numbers are accepted in the Profile Description string. • **Profile Action** - Select the status of profile action whether to allow or deny the channels associated with the specified profile. The default option is **Deny**. The list contains: – **Permit** – Specifies that channels associated with the profile is allowed. When the profile action is permit, the matching rule is executed. The IGMPv3 reports with specific source list are modified with the sources that are permitted.

- **Deny** – Specifies that channels associated with the profile is denied. When the profile action is deny, the matching rule is not found in the table. The client report is not processed.

  Profile Action can be changed only if the Profile Status is set as InActive.

- **Port Reference Count** - Displays the number of profile-to-port mappings configurations for the particular profile. A profile can be deleted only if there are no port reference counts. The default value is **0**.

- **Vlan Reference Count** - Displays the number of profile-to-VLAN mapping configurations for the entire system. A profile can be deleted only if the VLAN reference count is 0. The default value is **0**.

- **Profile Status** - Select the profile status of a row in the multicast profile table. New entries can be created in the multicast filter rule table and also the existing entries can be updated. The default option is **InActive**. The list contains:
  - **Active** – Specifies that the status of the specific row is active in the multicast profile table. When active, the profile is matched with the client report
  - **InActive** – Specifies that the status of the specific row is inactive in the multicast profile table.

Buttons

- **Add** - To add and save new configuration
- **Reset** - To reset to default value for respective fields and discard all user inputs.
- **Apply** - To modify attributes for the selected entry and save the changes.
- **Delete** - To delete the selected entry.

  A profile can be deleted only if the Port and Vlan reference count is 0.

- **Configure Trace Options -** To access **Tac Traces** screen

27.1.1 TAC Traces

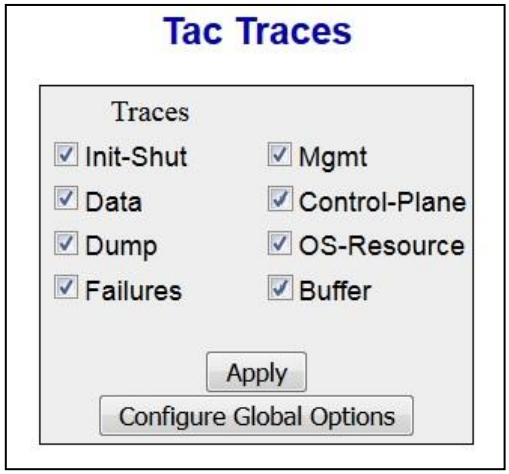


Figure 27-2 : Tac Traces

Screen Objective	This screen allows the user to enable the required debug statements that will be useful during debug operation. System errors such as memory allocation failures are notified by means of LOG messages and TRACE messages. Interface errors and protocol errors are notified by means of TRACE messages
Navigation	**Multicast** > **TAC** > **Profile >TAC Profile Configuration** screen **> click Configure Trace Options** button**.**
Fields	• **Traces** - Select the traces for which debug statements is to be generated. The list contains – **Init-Shut** – Generates debug statements for initialization and shutdown traces. This trace is generated on failure initialization, successful initialization and shutting down of TAC related module and memory – **Data** – Generates debug statements for Data Plane functionality traces. – **Dump** - Generates debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets. – **Failures** – Generates debug statements for any failures occurring. – **Mgmt** – Generates debug statements for Management Plane functionality traces. – **Control-Plane** – Generates debug statements for Control Plane functionality traces. – **OS-Resource** – Generates debug statements for Traces with respect to allocation and freeing of all resource expect the buffers. – **Buffer** - Generates debug statements for traces with respect to allocation and freeing of Buffer.

Buttons	• **Apply** - To modify attributes and save the changes. • **Configure Global Options -** To access the **Tac Profile Configuration** screen**.**

27.2 TAC Profile Filter Configuration

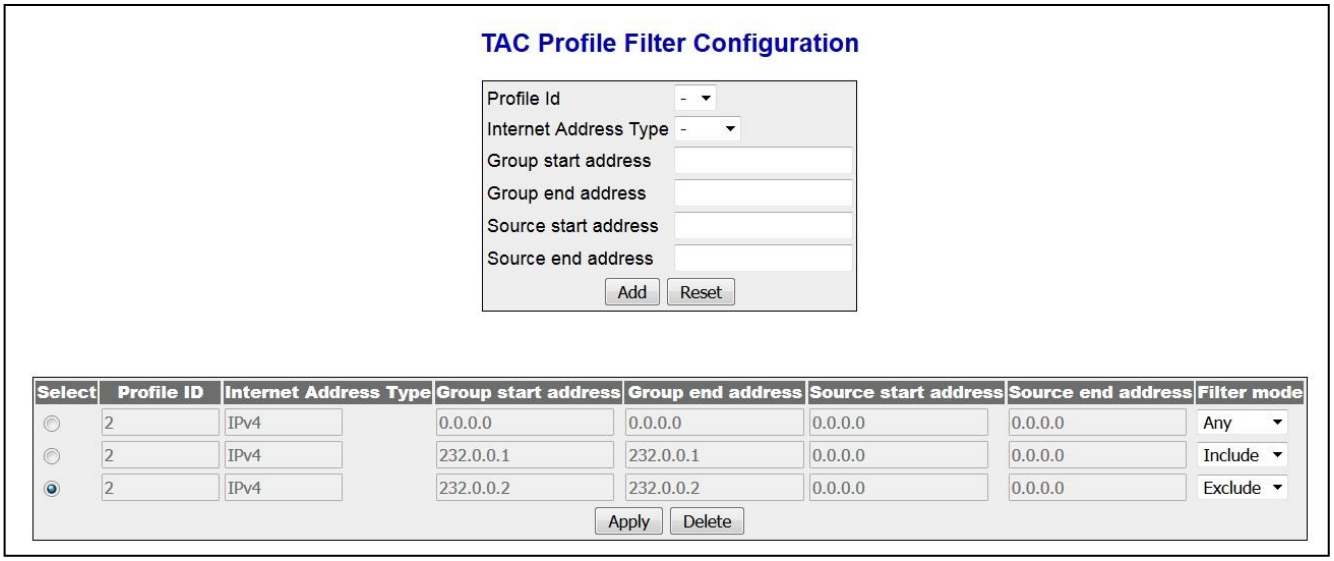


Figure 27-3 : TAC Profile Filter Configuration

Screen Objective	This screen specifies the packets for which the configuration needs to be enforced. A new rule for a particular profile is created based on the group and source address range. The rules are created and added in a RB Tree. The memory reserved for the rules are common for all the profiles.
☞	This screen can be configured only if TAC Profile is created and the profile status is set as InActive using the **TAC Profile Configuration** screen.
Navigation	**Multicast** > **TAC** > **Profile filters**
Fields	• **Profile Id** - Select the unique identifier for each multicast profile entry. This value ranges from 1 to 4294967295. ✎ This field lists the profile entries created using the **TAC Profile Configuration** screen. • **Internet Address Type** - Select the internet address type in the profile. The list contains: – **IPv4** - Sets the internet address type as IPv4. – **IPv6** - Sets the internet address type as IPv6.

The address type of the profile entry should match the address type set for the profile in the **TAC Profile Configuration** screen.

Group start address - Enter the multicast group address, which is the start of multicast group address range. It can be a particular multicast address or 0.0.0.0 which indicates that it is a wild card. To configure a specific address, both the start and end group address must be the same.

- **Group end address** - Enter the multicast group address, which is the end of multicast group address range.. This can be a particular multicast address or 0.0.0.0 which indicates that it is a wild card.

  To configure a specific address, both the start and end group address must be the same.

  The end address cannot be specific address if the start address is a wildcard (0.0.0.0).

- **Source start address** - Enter the multicast source address, which is the start of multicast group address range . This can be a particular IP address or 0.0.0.0 which indicates that it is a wild card. A filter rule with source address as wild card is used to filter based on groups.

  To configure a specific address, both the start and end source address must be the same.

- **Source end address** - Enter the multicast source address, which is the end of multicast group address. This can be a particular IP address or 0.0.0.0 which indicates that it is a wild card.

  To configure a specific address, both the start and end source address must be the same.

  The end address cannot be specific address if the start address is a wildcard (0.0.0.0).

- **Filter mode** - Select the type of packets to be filtered. The default option is **Any**. The list contains:
  - Include – Specifies that filter is applied to include IGMP/MLD reports.
  - Exclude – Specifies that the filter is applied to exclude IGMP/MLD reports.
  - Any – Specifies that the filter is for all the packets.

Buttons

- **Add** - To add and save new configuration.
- **Reset** - To reset to default value for respective fields and discard all user inputs.
- **Apply** - To modify attributes for the selected entry and save the changes.
- **Delete** - To delete the selected entry.

Chapter 27

Serial Data I/O

The **AMG 9IM2x/9HM2x** series of Multi Port Ethernet Switches also support built-in I/O ports. These I/O ports allow serial data ports, alarm contacts, audio devices and analogue video to be directly connected to the switch.

AMG 9IM2x/9HM2x web management interface has the provision to configure these I/O features and facilitate connectivity of low speed I/O devices.

The left navigation pane only has I/O menu when serial data ports are present in the device. Number of serial data I/O in configuration/status pages corresponds to serial data I/O present in the device.

Web pages corresponding to I/O ports are available only when device is configured with serial data ports.

To access Serial data I/O screens, click **I/O > Serial**

The **Serial Data** parameters are configured through the screens displayed by the following tabs:

- Serial Data
- Serial IP

By default the tab **Serial Data** displays the **Serial Port Settings** screen.

There are three examples of typical use cases of Serial IO :

- Point-to-point
- Multiple point-to-point
- Point to multipoint

28.1 Serial Data Applications

Serial data over IP application

The serial data over IP application can be used in several ways, but the use cases can be divided into three typical applications :

- Point-to-point
- Point-to-multipoint (typically a master-slave application)
- PC access to remote serial devices. (virtual COM port)

Serial data point-to-point

In this way two serial devices can communicate over an IP network as two peers using UDP.

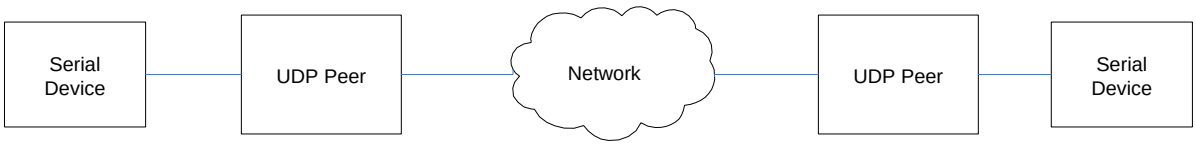


Figure 28-1 : Serial Data Point to Point

Point-to-multipoint (broadcast / unicast)

This allows one serial device (typically a master) to communicate with multiple serial devices using UDP transport. It can be set up as IP broadcast, or via multiple IP unicast streams.

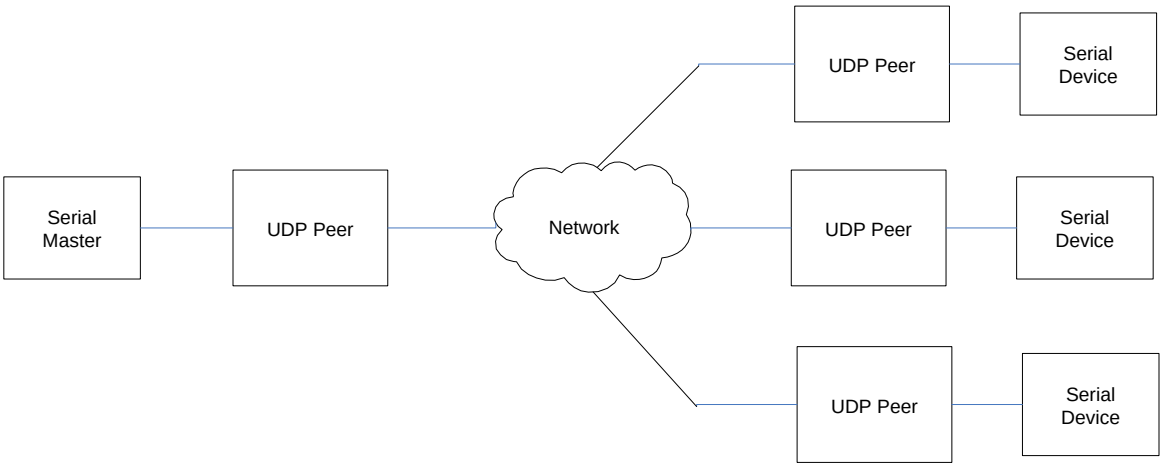


Figure 28-2 : Serial Data Point-to-Multipoint

Serial Port Re-director (Virtual Serial Port)

By using serial port redirector software, an application can access remote serial devices as if they were directly connected to the PC. AMG can provide a Serial Port Re-director (PC) application that allows up to 32 virtual serial ports to be created. There is also the possibility for an application to directly connect to the Serial over IP.

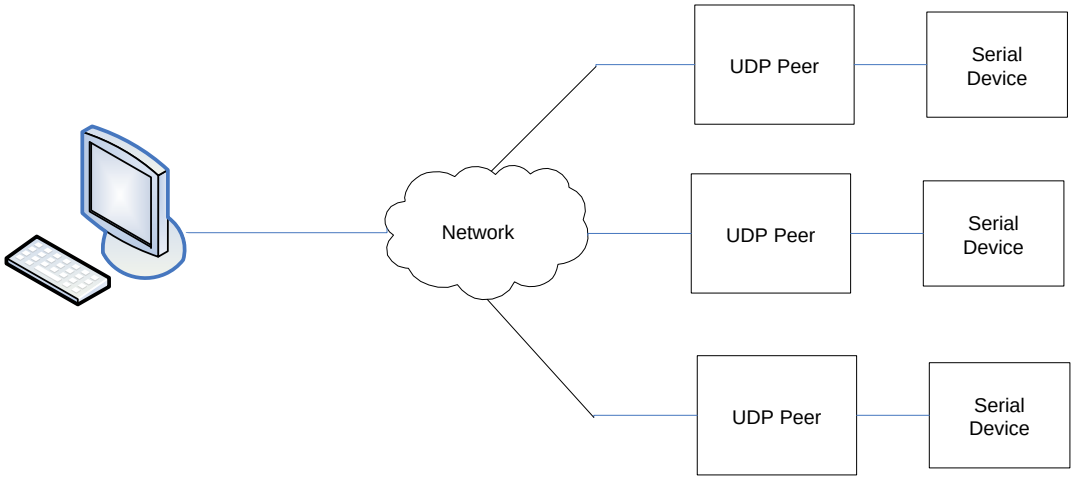


Figure 28-3 : Serial data port re-director

28.2 Serial Data Port Configuration

AMG 9IM2x/9HM2x web management interface supports configuring serial port parameters such as serial port type, speed, number of data bits, number of stop bits etc.

The following web page shows 4 channels of data D1-D4.

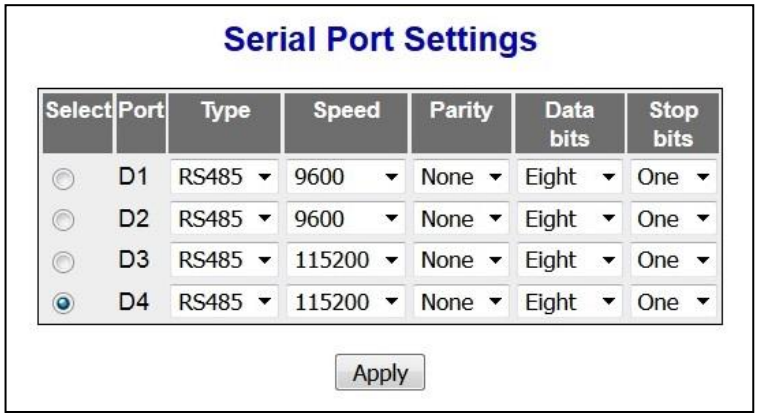


Figure 28-4 : Serial Data Port Settings D1-D4

Screen Objective	This screen is used to configure serial data port parameters for the serial ports on this device.
Navigation	**I/O > Serial > Serial Data**
Fields	• **Select** - the serial port to configure • **Port** - the serial port name • **Type** - to configure/view the mode in which serial port to be/is operational. • **Speed** - to configure baud rate at which serial port to be operated. • **Parity** - to set parity bit in each character transferred over serial port. • **Data Bits** - to configure the number of data bits in each character transferred over serial port. • **Stop bits** - to configure number of stop bits to be sent in each character transferred over serial port.
Buttons	• Apply - button to apply configured changes to device.

28.3 Serial Data IP Configuration

Serial data across AMG 9IM2x/9HM2x devices is transferred through serial data ports using IP protocol. AMG 9IM2x/9HM2x web management interface gives provision to configure IP address and UDP port number of AMG 9IM2x/9HM2x device that is involved in data transfer.

AMG 9IM2x/9HM2x devices can be configured for point-to-point data transfer as well as broadcast type of data transfer through web management interface.

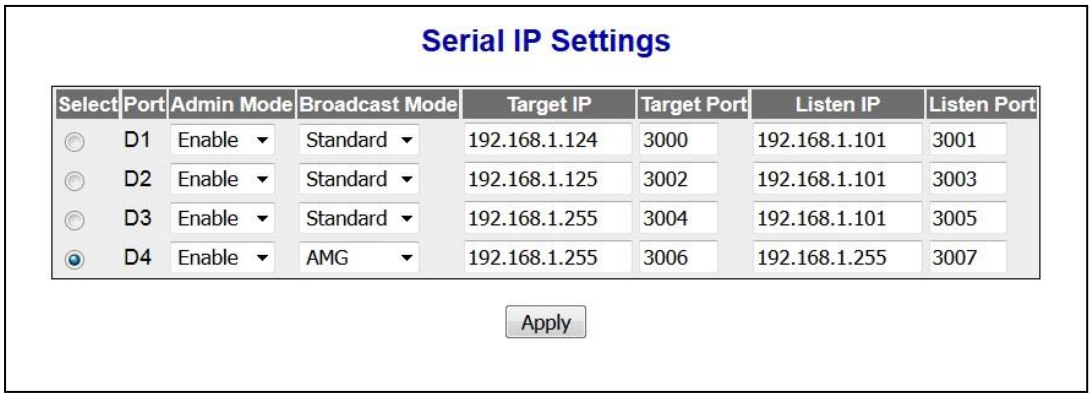


Figure 28-5 : Serial Data Port - IP configuration

Screen Objective	Use this page to configure the remote transmission and reception of network traffic to and from serial ports.
Navigation	**I/O > Serial > Serial I/P**
Fields	• **Select** - the particular serial port to configure • **Admin Mode** - to enable the serial port for UDP/IP communication. If this field is not enabled, the switch will not transmit or receive any serial data related messages via UDP/IP to or from the remote device on the network. – **Enable** - enables the serial port – **Disable** - disables the serial port • **Broadcast Mode** - select between the following broadcast modes. These must be used together with a Broadcast Target Address e.g. 192.168.1.255. – **Standard** – Broadcast packets with the standard broadcast MAC address FF:FF:FF:FF:FF:FF will be sent. Use this mode for communication with standard devices on the network, such as the **AMG9IM2x/9HM2x** Ethernet Switch or **AMG7100** Video Encoder. – **AMG** - Broadcast packets with a proprietary MAC address will be sent. Use this mode for communication with remote M-SES switches which do not accept standard broadcast packets, such as the early generation **AMG9024GM-H-2S2I8C-R** Ethernet Switch.

- **Dual** – Both Standard and AMG broadcast packets will be sent. Use this mode for communication with a mixture of standard and M-SES devices.

- **Target IP** - the IP address for that particular serial port to send data to.
- **Target Port** - the layer-4 port number for that particular serial port to send data to.
- **Listen IP** - the IP address for that particular serial port to listen for data.

  This value should either be the IP address of the M-SES that is being configured, or a broadcast address ending in 255 for example xxx.xxx.xxx.255

- **Listen Port** - the Layer-4 port number for that particular serial port to listen on, for data.

Buttons	• Apply - button to apply configuration changes to device.

28.4 Serial Data Example A : Point-to-point

AMG9024GM-H-2S2I8C-R: 4 Data channels D1-D4 <--> D1-D4
M-SES 1, 2: D1-D4: RS232, 9600bps

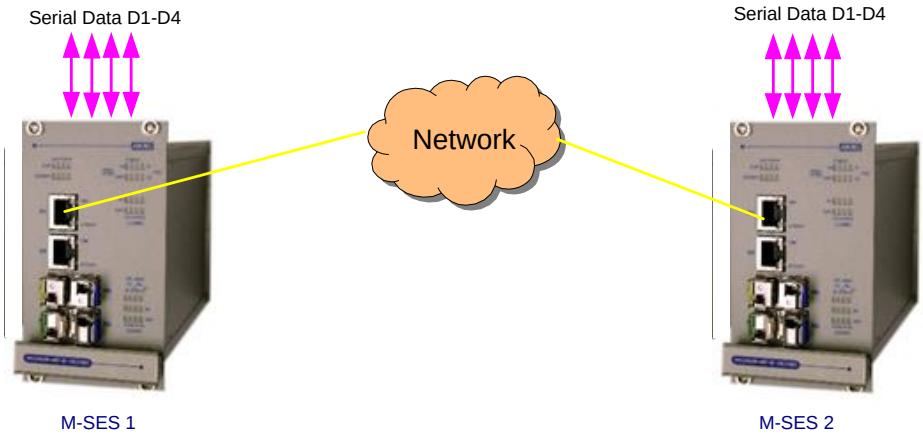


Figure 28-6 : Serial data point-to-point unicast

Serial Data Port Settings D1-D4

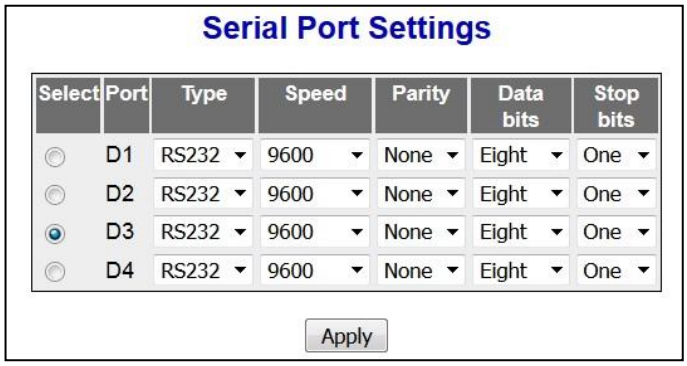


Figure 28-7 : Serial Data Port Settings M-SES 1,2

Serial Data IP Settings M-SES 1

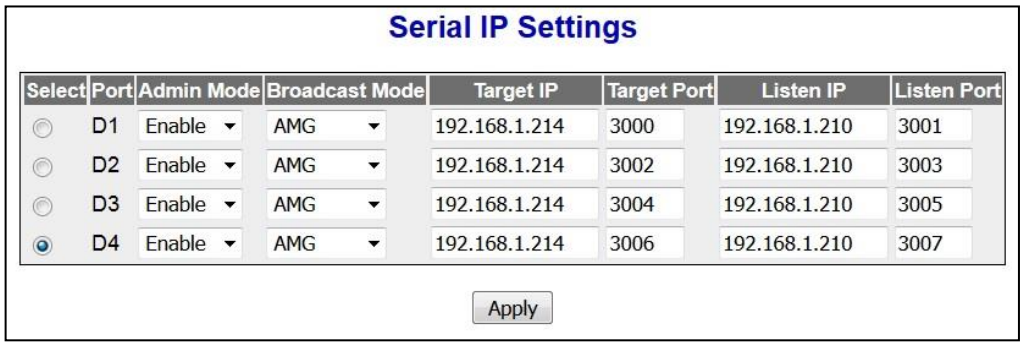


Figure 28-8 : Serial Data Port Settings M-SES 1

Serial Data IP Settings M-SES 2

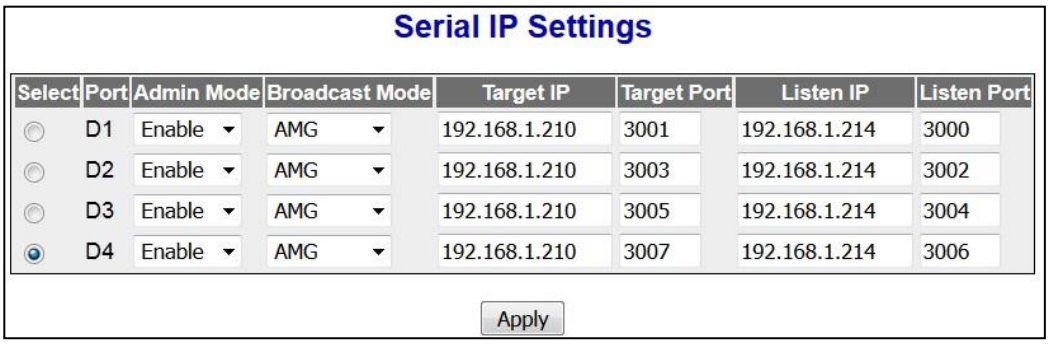


Figure 28-9 : Serial Data Port Settings M-SES 2

28.5 Serial Data Example B : Multiple point-to-point

AMG9024GM-H-2S2I8C-R (4 Data channels D1...D4) to 4x **AMG9024GM-H-2S4C-R**

i.e. M0/D1 <--> M1/D1, M0/D2 <--> M2/D1, M0/D3 <--> M3/D1, M0/D4 <--> M4/D1

- M-SES 0: D1-D4: RS485, 115.2kbps,
- M-SES 1…4: D1, D2: RS485, 115.2kbps

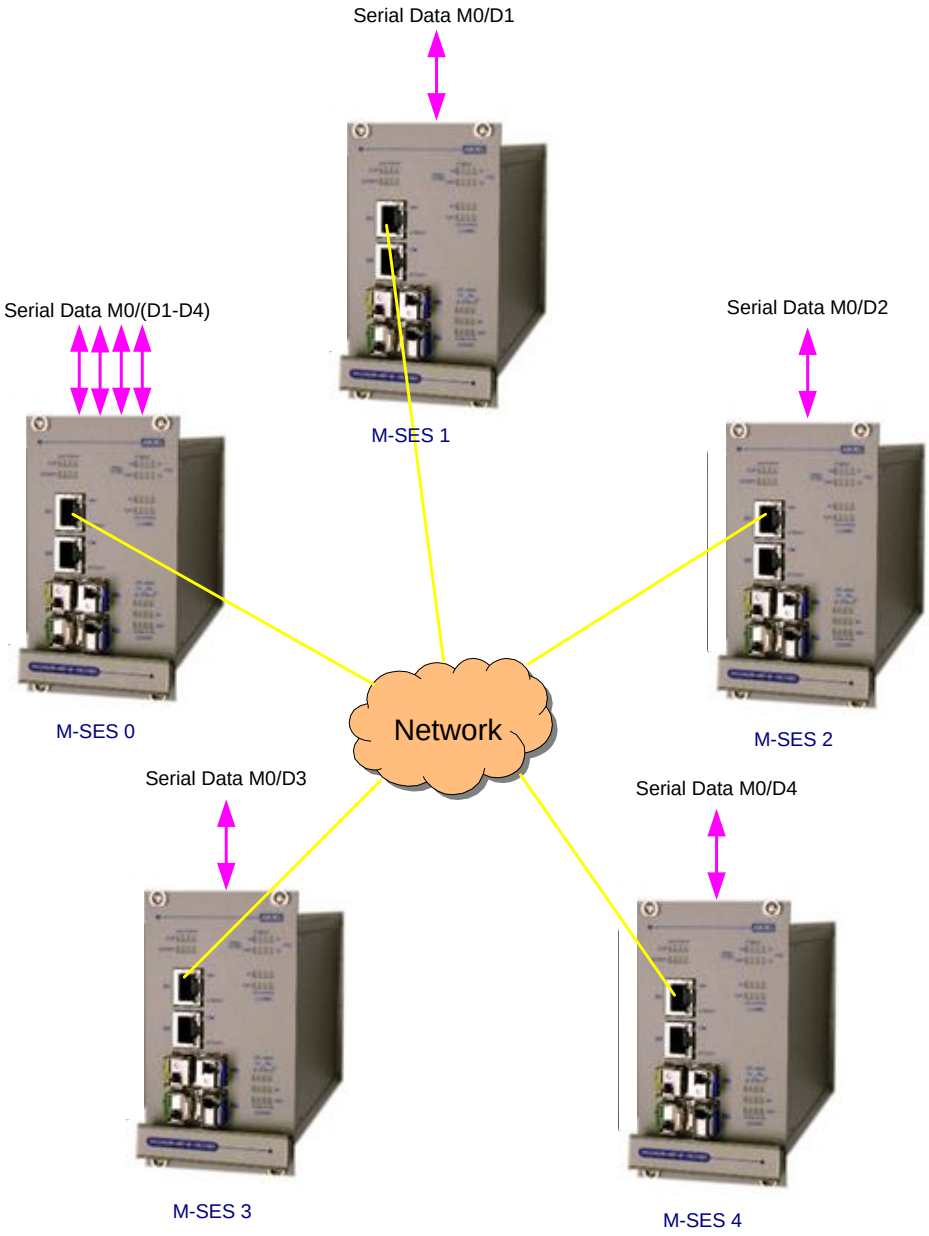


Figure 28-10 : Serial data multiple point-to-point (unicast)

Serial Data Port Settings M-SES 0

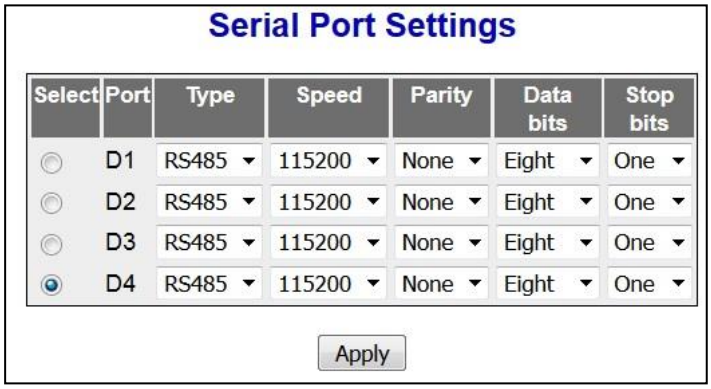


Figure 28-11 : Serial Data Port Settings M-SES 0

Serial Data IP Settings M-SES 0

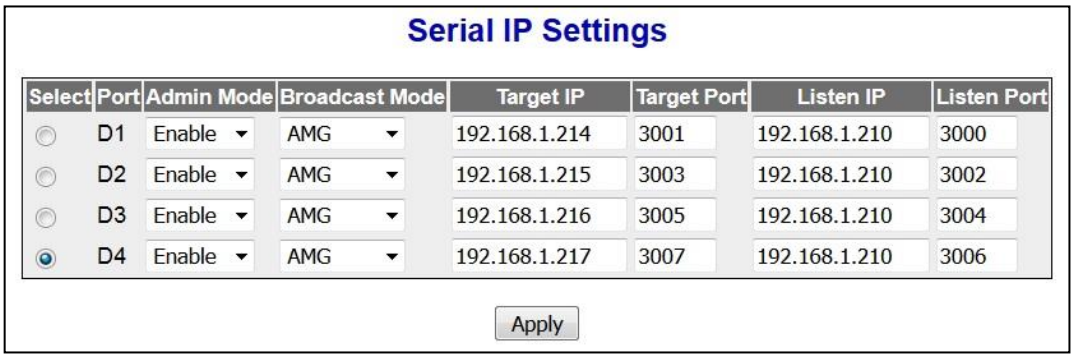


Figure 28-12 : Serial Data IP Settings M-SES 0

Serial Data Port Settings M-SES 1-4

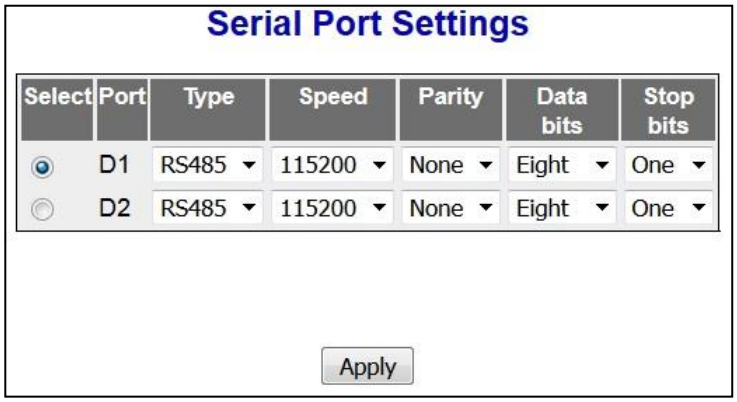


Figure 28-13 : Serial Data Port Settings M-SES 1-4

Serial Data IP Settings M-SES 1

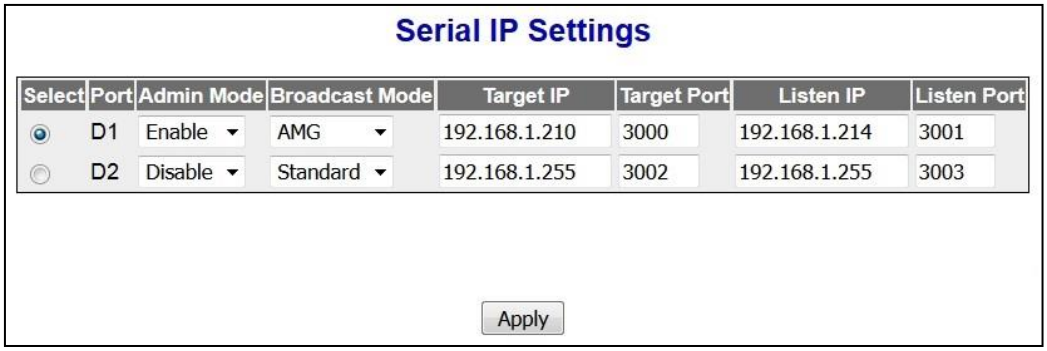


Figure 28-14 : Serial Data IP Settings M-SES 1

Serial Data IP Settings M-SES 2

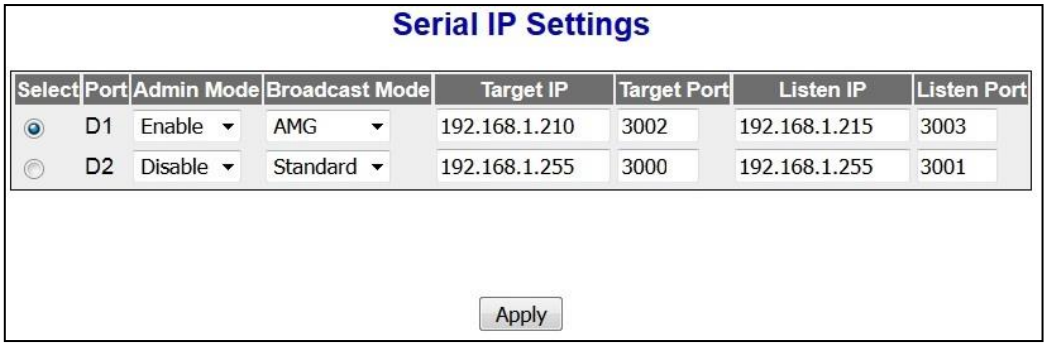


Figure 28-15 : Serial Data IP Settings M-SES 2

Serial Data IP Settings M-SES 3

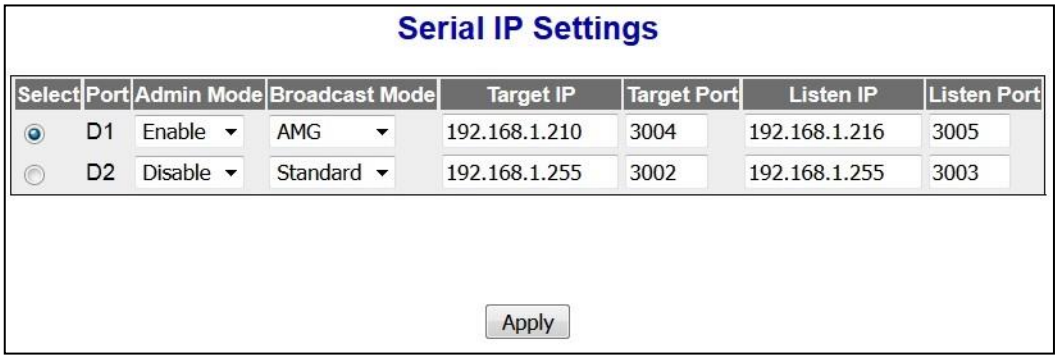


Figure 28-16 : Serial Data IP Settings M-SES 3

Serial Data IP Settings M-SES 4

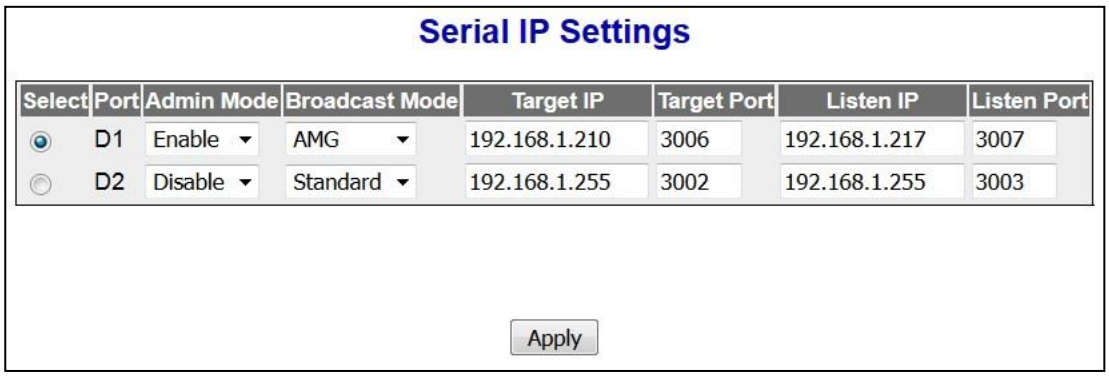


Figure 28-17 : Serial Data IP Settings M-SES 4

28.6 Serial Data Example B : Point-to-multipoint

Master to VE Slaves Broadcast, VE Slaves to Master Unicast

AMG9024GM-H-2S4C-R (2 Data channels D1, D2) to 4x **AMG9024GM-H-VE-R**
(1 data channel used on each M-SES Video Encoder).

i.e. M0/D1 <--> M1/D1, M2/D1
M0/D2 <--> M3/D1, M4/D1

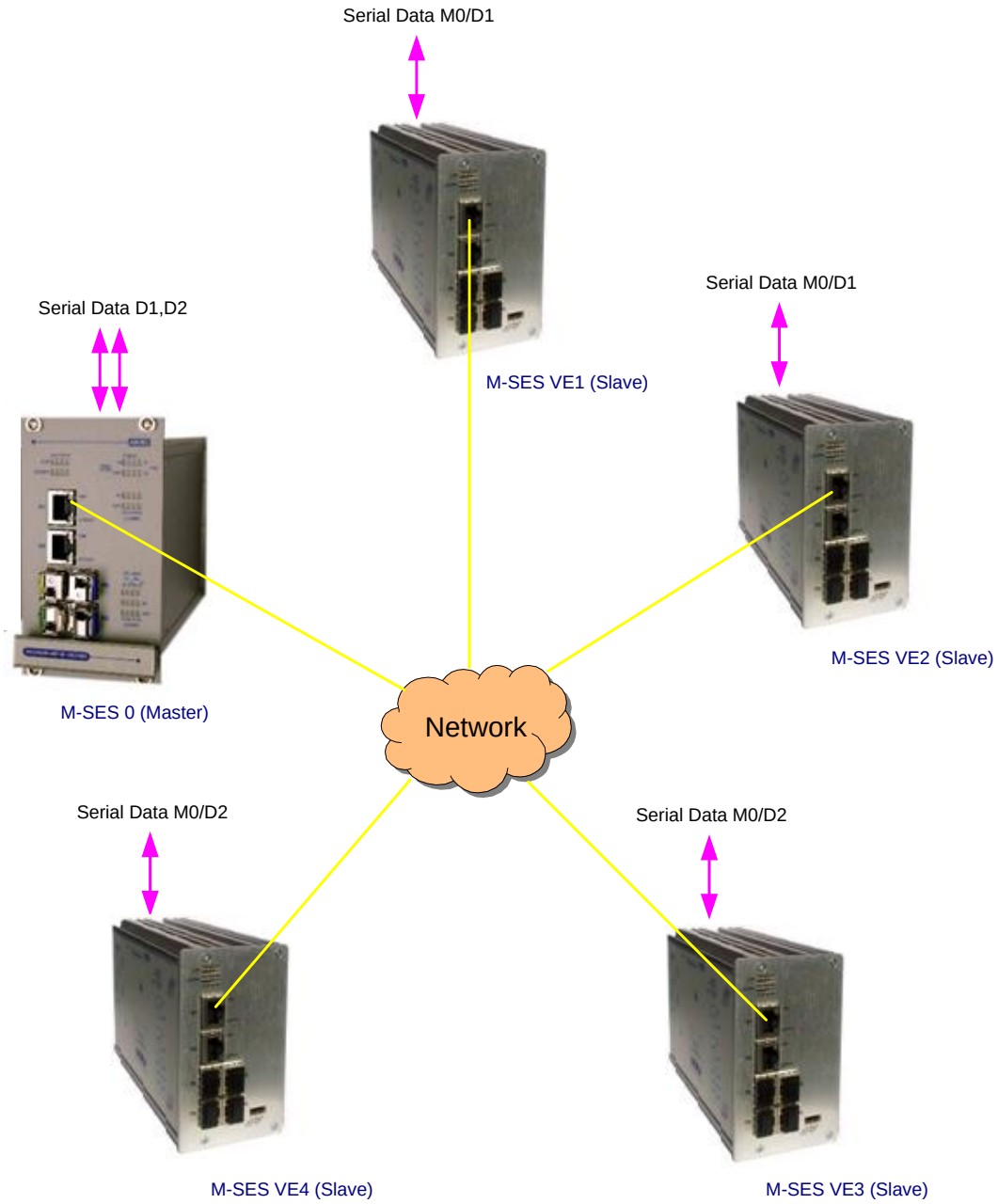


Figure 28-18 : Serial Data point-to-multipoint

Serial Data Port Settings M-SES 0

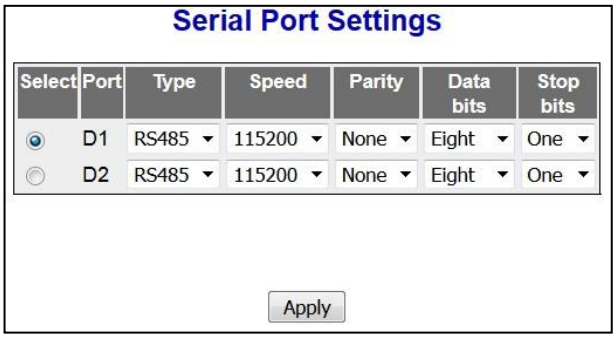


Figure 28-19 : Serial Data Port Settings M-SES 0

Serial Data IP Settings M-SES 0

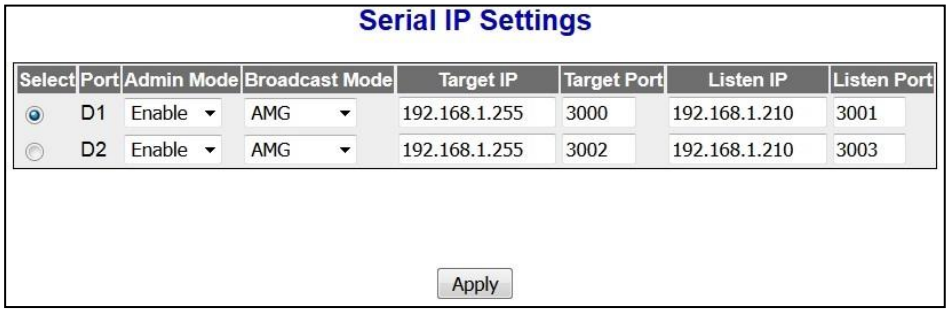


Figure 28-20 : Serial Data IP settings M-SES 0

Serial Data Port & IP Settings VE 1,2

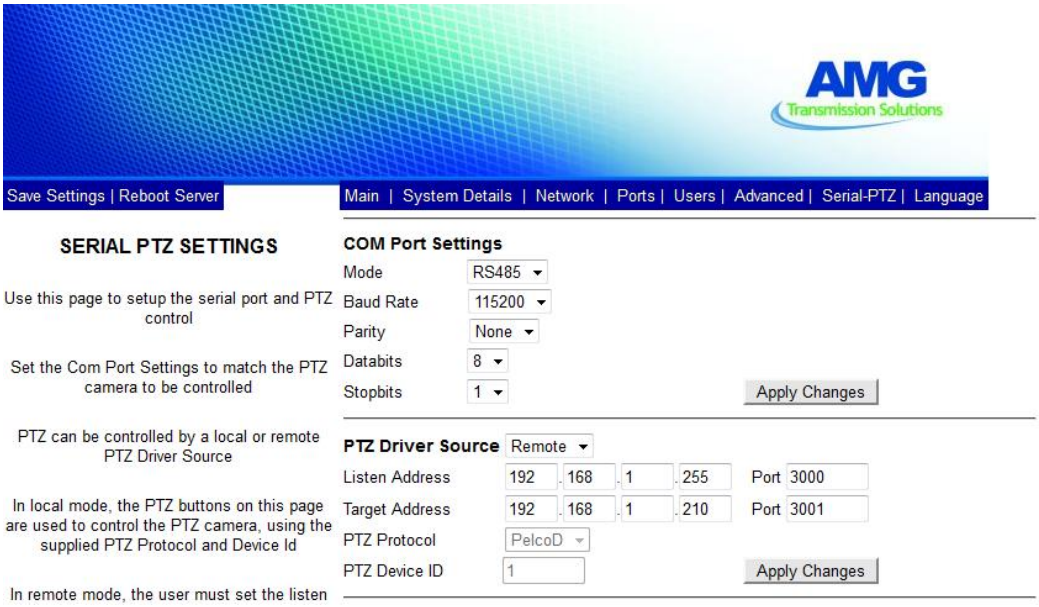


Figure 28-21 : Serial Data Port & IP settings VE 1,2

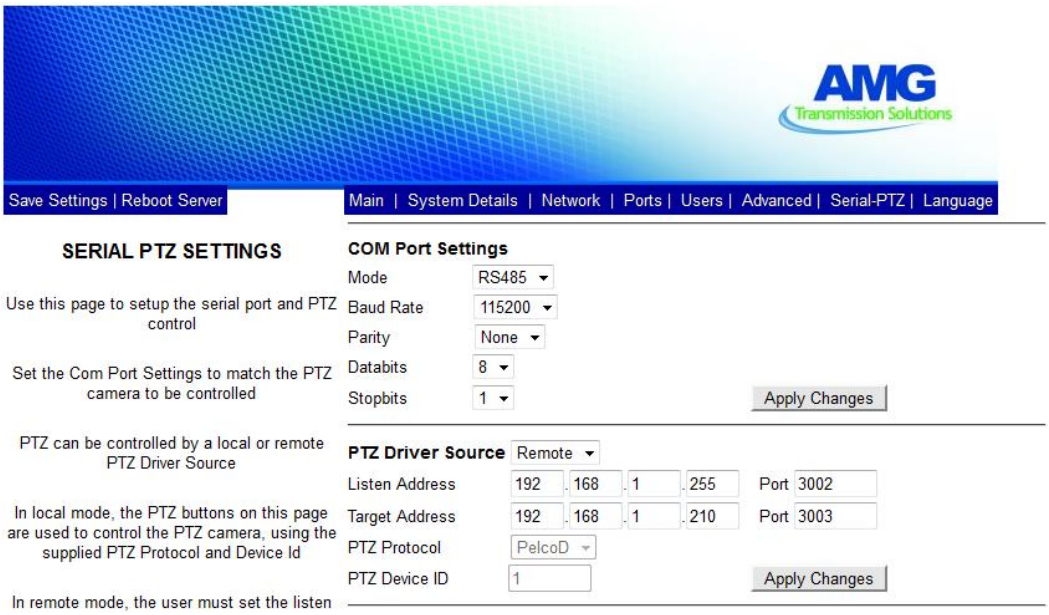


Figure 28-22 : Serial Data Port & IP settings VE 3,4

Chapter 28

Contact Closure I/O over IP

The **AMG 9IM2x/9HM2x** series of Multi Port Ethernet Switches also support built-in I/O ports. These I/O ports allow serial data ports, alarm contacts, audio devices and analogue video to be directly connected to the switch.

AMG 9IM2x/9HM2x web management interface has the provision to configure these I/O features and facilitate connectivity of low speed I/O devices.

Web pages corresponding to I/O ports are available only when device is configured with serial data / contact closure data ports.

The navigation pane only has I/O menu when serial data / contact closure ports are present in the device. Number of contact closures in configuration/status pages correspond to contact closures present in the device.

To access contact closures I/O screens, click **I/O > Contact Closures**

There are four examples of use cases of contact closures IO :

- Point-to-point
- Multiple point-to-point
- Point to multipoint
- Multipoint-to-point

29.1 Contact Closures Applications

The Contact Closures I/O over IP application can be used in several ways, but the use cases can be divided into three typical applications:

- Point-to-Point
- Point-to-Multipoint (typically a master-slave application)
- Multipoint-to-Point "OR”ing (unicast or broadcast)

Contact Closures Point to Point

When each AMG 9IM2x/9HM2x Contact Closure input is mapped (over IP) to a Contact Closure output on one AMG 9IM2x/9HM2x switch (Unicast), a single input controls a single output.

Contact Closures Point-to-multipoint (broadcast / unicast)

When an AMG 9IM2x/9HM2x Contact Closure input is mapped (over IP) to a Contact Closure output on more than one AMG 9IM2x/9HM2x switch (Broadcast), a single input controls one output on several AMG 9IM2x/9HM2x switches.

Multipoint-to-Point "OR”ing

When more than one Contact Closure input is mapped (over IP) to a Contact Closure output (Multiple Unicast or Multiple Broadcast), the output is effectively controlled by more than one AMG 9IM2x/9HM2x . In this case the value of each Contact Closure input is logically “OR”d with all other corresponding Contact Closure inputs for this output.

This means that ANY AMG 9IM2x/9HM2x Contact Closure input can turn a corresponding Contact Closure output ON, but ALL incoming Contact Closure inputs must be OFF before the Contact Closure output is turned OFF.

29.2 Contact Closure Configuration

Contact Closure inputs & outputs of AMG 9IM2x/9HM2x devices are transferred through IP protocol. AMG 9IM2x/9HM2x web management interface gives provision to configure I/O participation and destination IP address(s) of AMG 9IM2x/9HM2x device that are involved in this control.

AMG 9IM2x/9HM2x devices can be configured as point-to-point, point-to-multipoint or multipoint-to-point (with logical “OR”ing function) control through web management interface.

AMG 9IM2x/9HM2x web management interface has provision to configure input enable, target IP address and output mode / enable of contact closure.

Each Contact Closure channel may be configured either as input or output.

The following web page shows 16 channels of Contact Closure I/O.

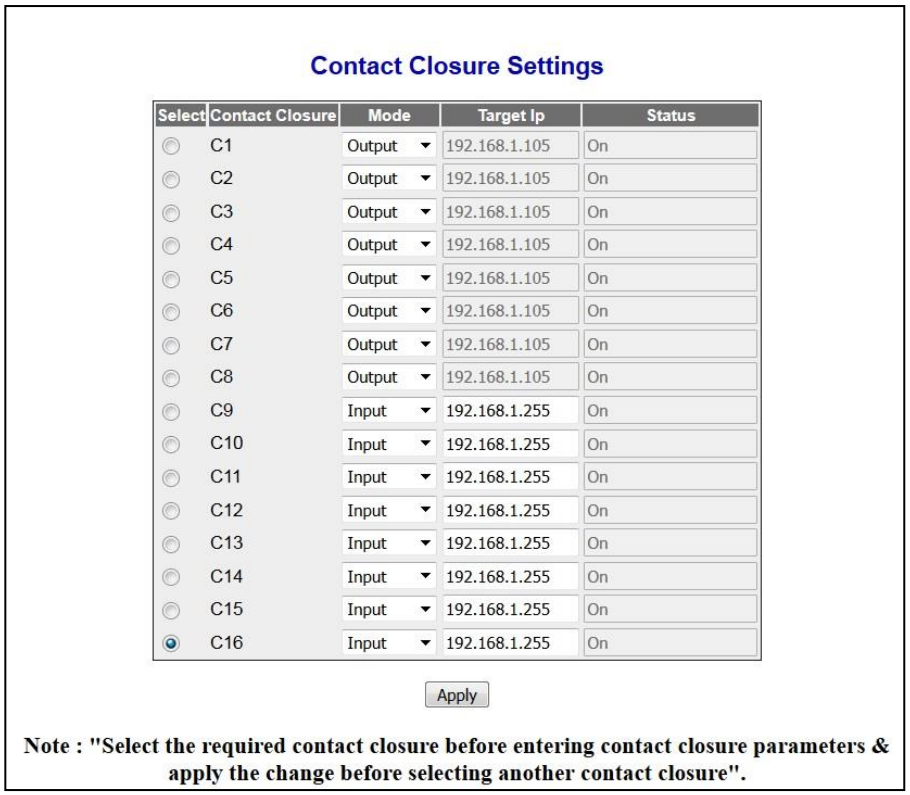


Figure 29-1 : Contact Closure I/O - 16 channels

Screen Objective	This screen is used to configure serial data port parameters for the serial ports on this device.
Navigation	**I/O > Contact Closures**
Fields	• **Select** - the contact closure port to configure • **Contact Closure** - the contact closure port being configured • **Mode** - to enable a contact closure input or output. If this field is not enabled, the switch will not transmit or receive the contact closure information to / from remote device on the network. – **Input** - enables contact closure as an input – **Output** - enables the contact closure as an output – **Disabled** - disables contact closure input / output • **Target IP** - the IP address to which the status of that particular contact closure port input needs to be sent to. This value should either be the IP address of the target device, or a broadcast address ending in 255. For example xxx.xxx.xxx.255
Buttons	• Apply - button to apply configured changes to device.

29.3 Contact Closure Example A : Point-to-point

2x **AMG9024GM-H-2S2I8C-R**

8 Contact Closure channels C1-C8 <--> C1-C8

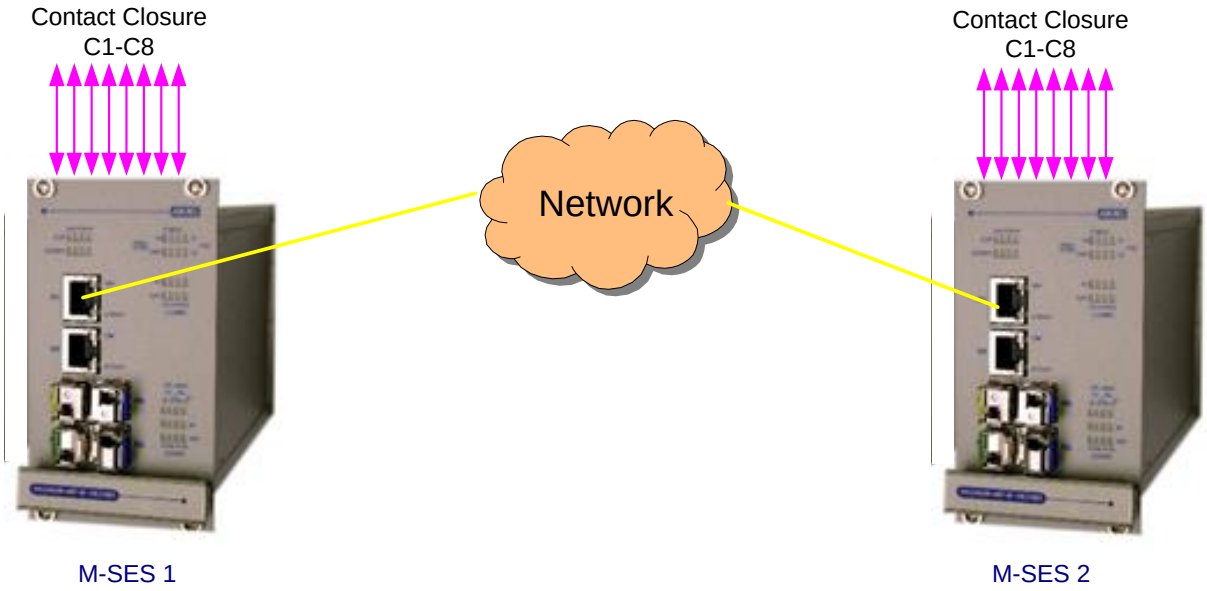


Figure 29-2 : Contact Closure point-to-point

Contact Closure Settings M-SES 1

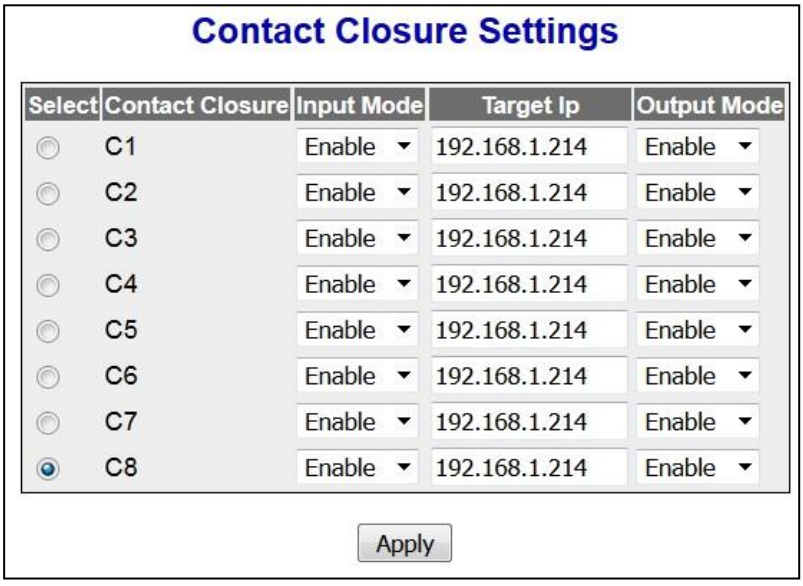


Figure 29-3 : Contact Closure Settings M-SES 1

Contact Closure Settings M-SES 2

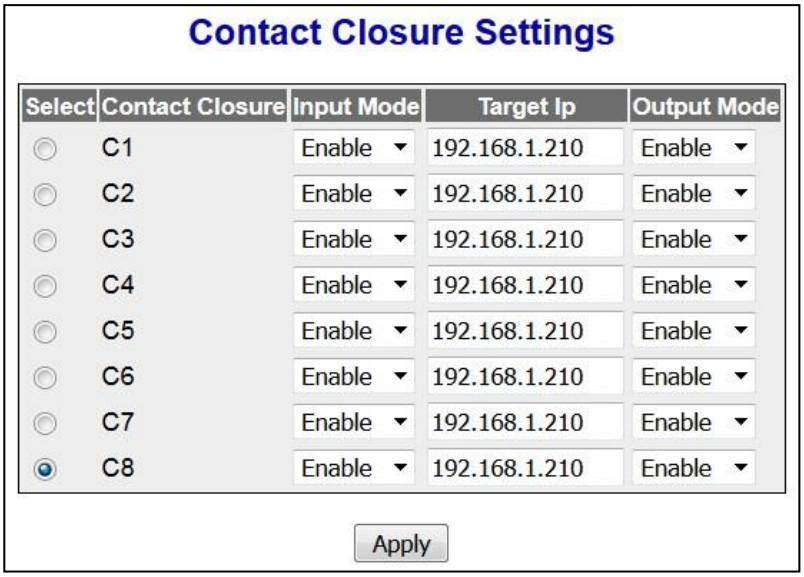


Figure 29-4 : Contact Closure Settings M-SES 2

29.4 Contact Closure Example B : Multiple point-to-point

AMG9024GM-H-2S2I8C-R (8 CC channels C1...C8) to
4x **AMG9024GM-H-2S4C-R:** A,B,C,D (2 CC channels used on each M-SES)

			M-SES A	M-SES B	M-SES C	M-SES D
		Chan	1	2	3	4
M-SES 1	<>	1	*			
	<>	2	*			
	<>	3		*		
	<>	4		*		
	<>	5			*	
	<>	6			*	
	<>	7				*
	<>	8				*

Table 29-1 : Contact Closure multiple point-to-point matrix

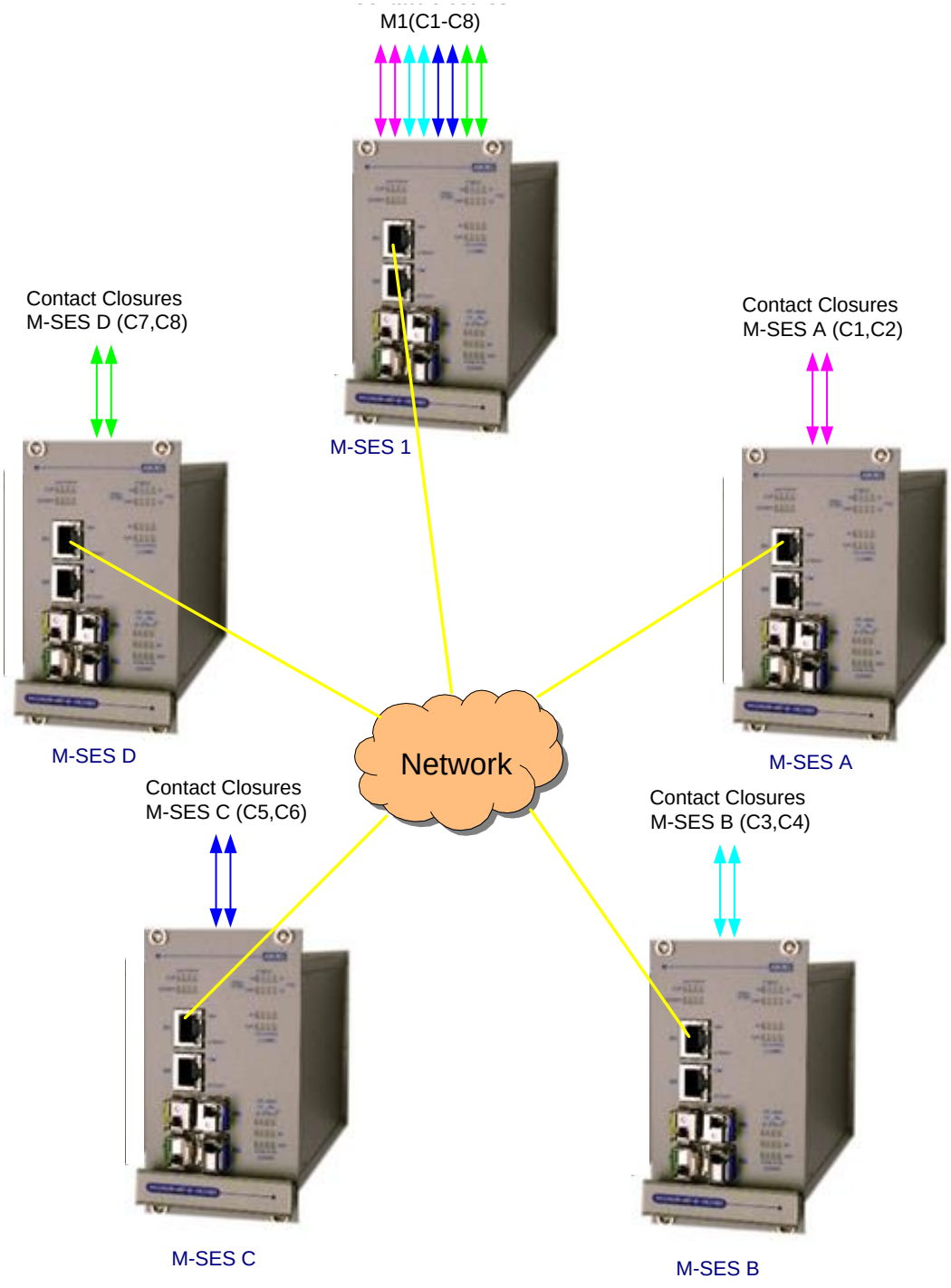


Figure 29-5 : Contact Closure multiple point-to-point

Contact Closure Settings M-SES 1

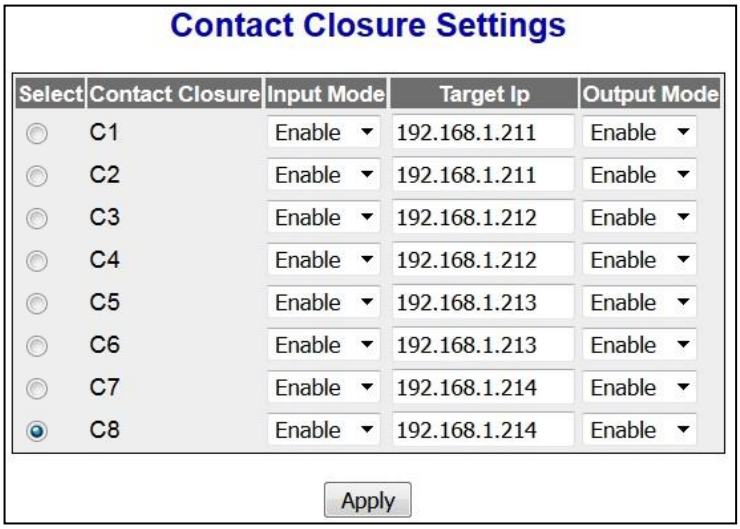


Figure 29-6 : Contact Closure Settings M-SES 1

Contact Closure Settings M-SES A

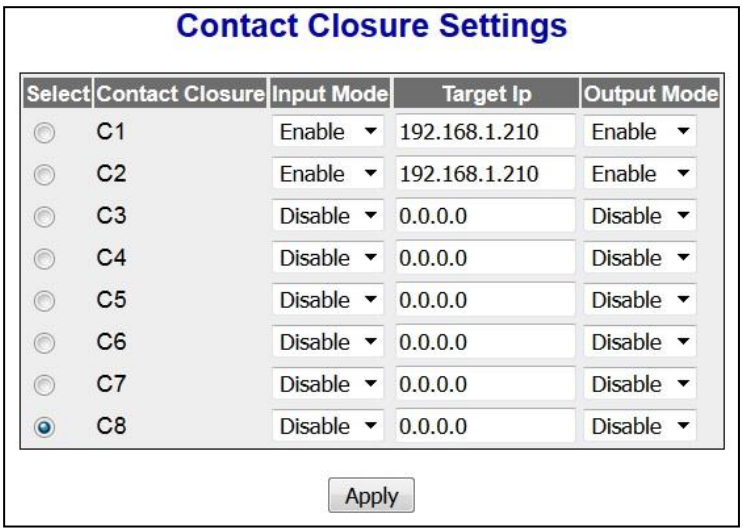


Figure 29-7 : Contact Closure Settings M-SES A

Contact Closure Settings M-SES B

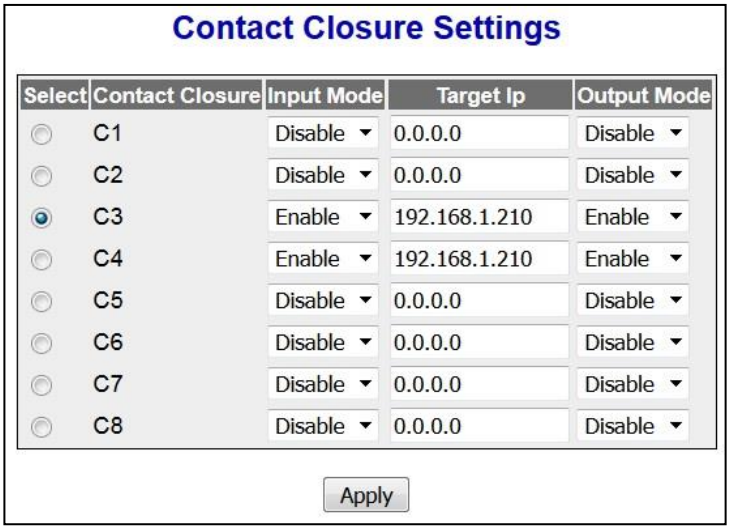


Figure 29-8 : Contact Closure Settings M-SES B

Contact Closure Settings M-SES C

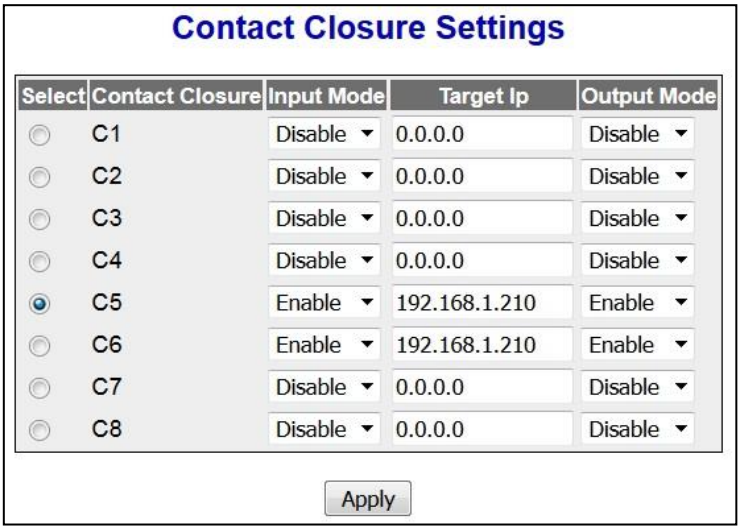


Figure 29-9 : Contact Closure Settings M-SES C

Contact Closure Settings M-SES D

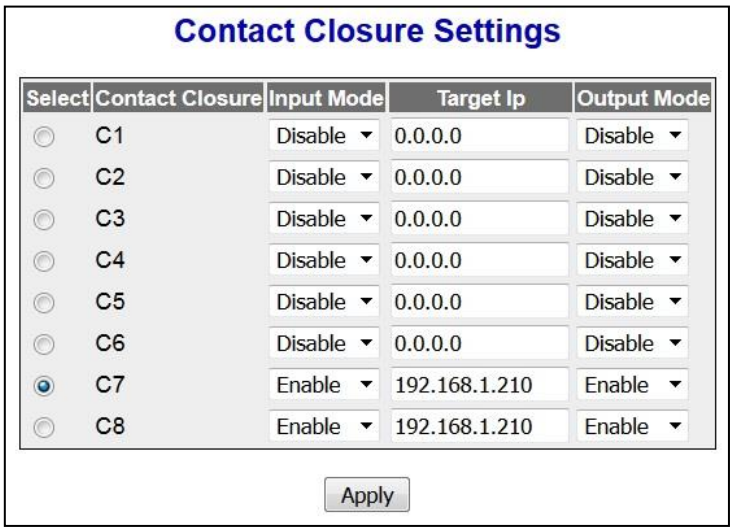


Figure 29-10 : Contact Closure Settings M-SES D

29.5 Contact Closure Example C : Point-to-multipoint

AMG9024GM-H-2S2I8C-R (8 CC channels C1...C8) to
4x **AMG9024GM-H-2S4C-R:** A,B,C,D (2 - 4 CC channels used on each M-SES)

			M-SES A	M-SES B	M-SES C	M-SES D
		Chan	1	2	3	4
M-SES 1	>>	1	*	*	*	*
	>>	2	*	*	*	*
	<>	3	*			
	<>	4		*		
	<>	5			*	
	<>	6			*	
	<>	7				*
	<>	8				*

Table 29-2 : Contact Closure point-to-multipoint matrix

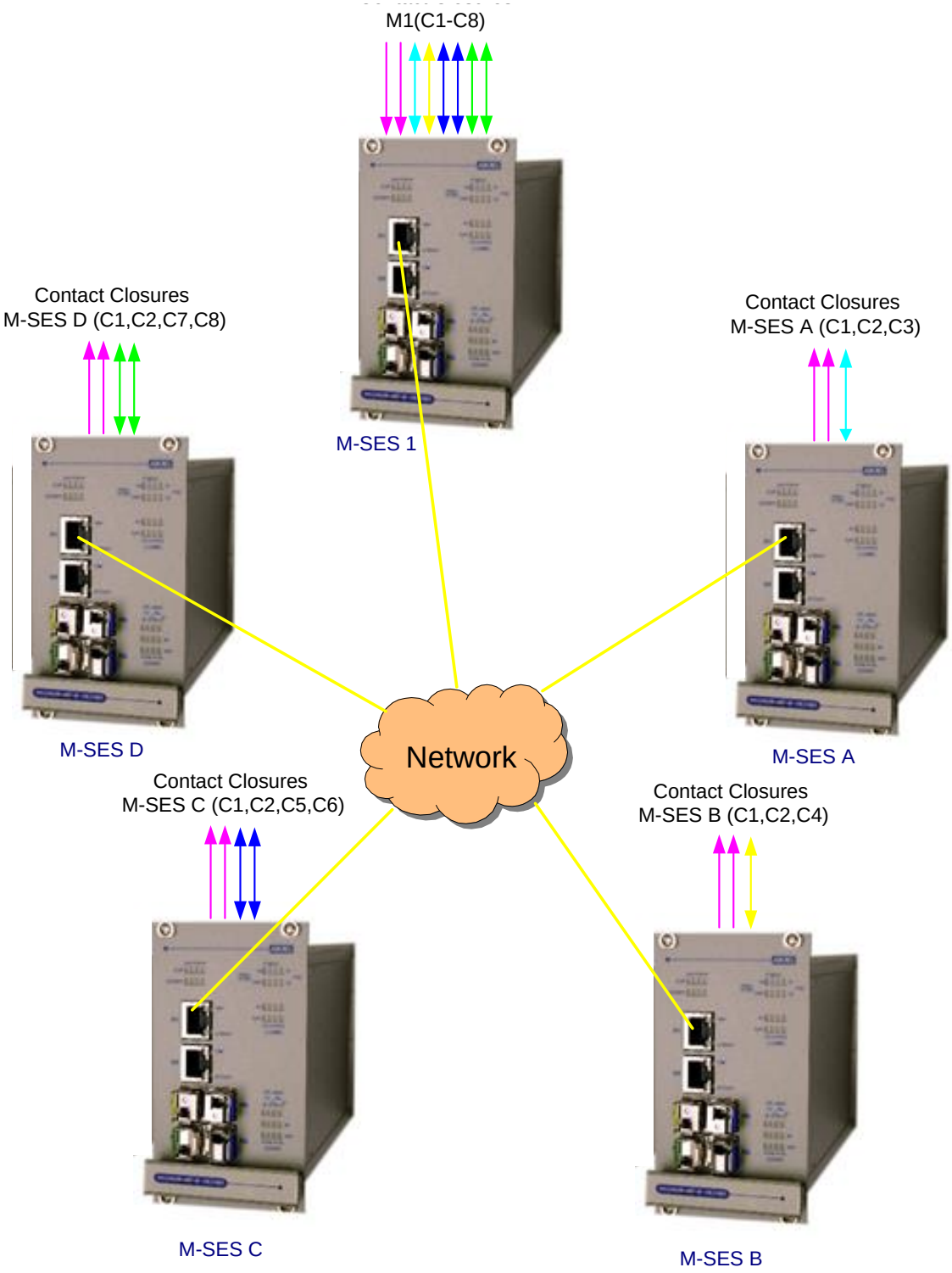


Figure 29-11 : Contact Closure point-to-multipoint

Contact Closure Settings M-SES 1

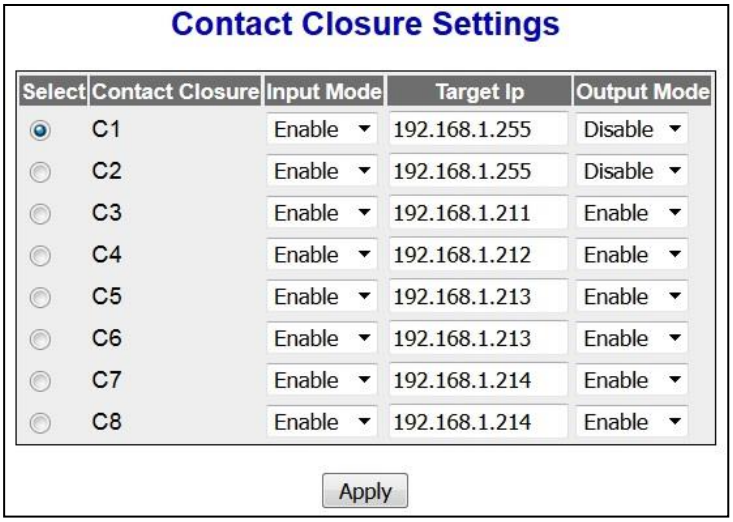


Figure 29-12 : Contact Closure Settings M-SES 1

Contact Closure Settings M-SES A

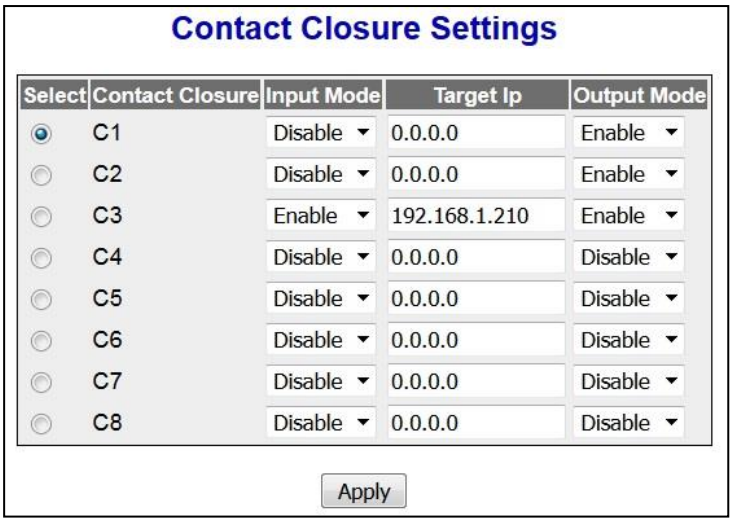


Figure 29-13 : Contact Closure Settings M-SES A

Contact Closure Settings M-SES B

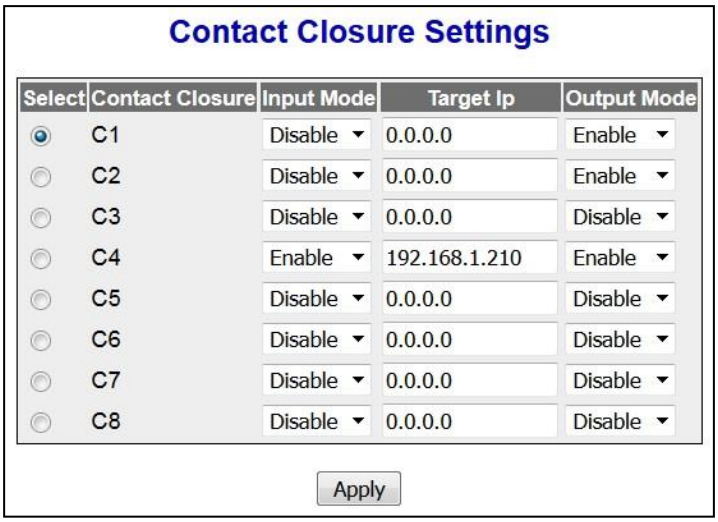


Figure 29-14 : Contact Closure Settings M-SES B

Contact Closure Settings M-SES C

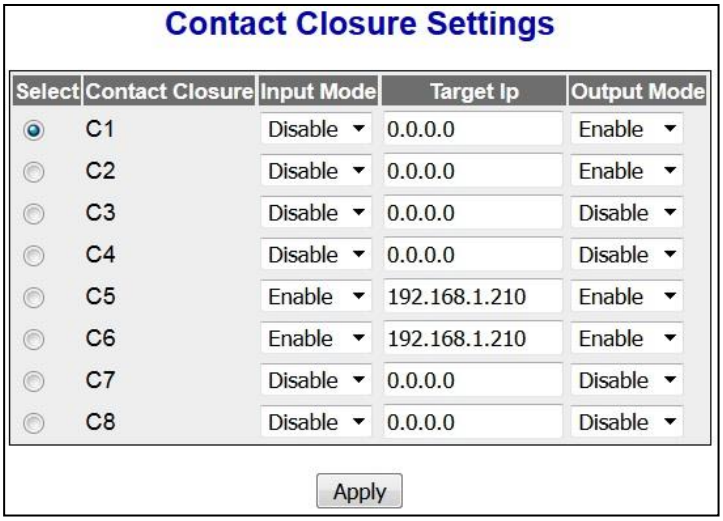


Figure 29-15 : Contact Closure Settings M-SES C

Contact Closure Settings M-SES D

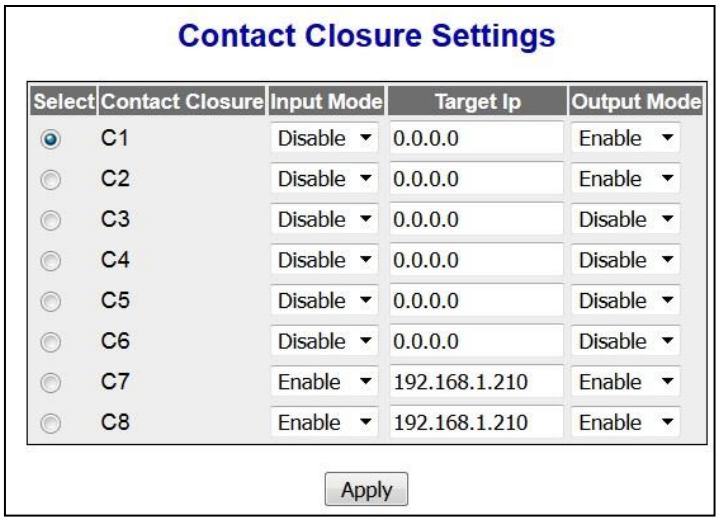


Figure 29-16 : Contact Closure Settings M-SES D

29.6 Contact Closure Example D : Multipoint-to-point

Broadcast, unicast “OR”ing

1x AMG9024GM-H-2S2I8C-R (8 CC channels C1...C8) to 4x **AMG9024GM-H-2S4C-R:** A,B,C,D (2,4 or 5 CC channels used on each M-SES)

			M-SES A	M-SES B	M-SES C	M-SES D
		Chan	1	2	3	4
M-SES 1	<OR>	1	*	*		
	<OR>	2	*	*		
	<OR>	3	*	*		
	<OR>	4	*	*		
	<OR>	5			*	*
	<OR>	6			*	*
	<>	7	*			
	<>	8		*		

Table 29-3 : Contact Closure multipoint-to-point matrix

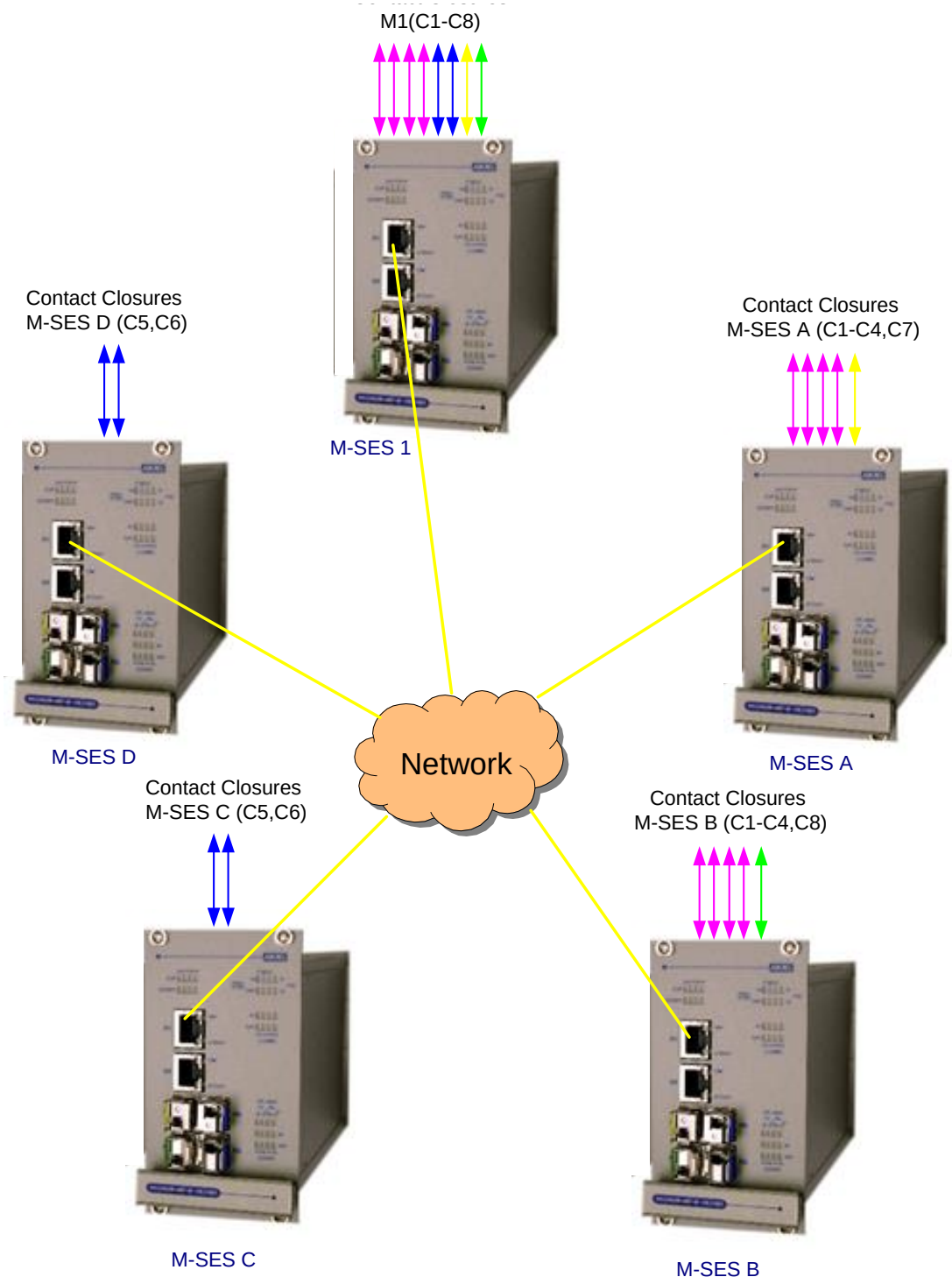


Figure 29-17 : Contact Closure multipoint-to-point

Contact Closure Settings M-SES 1

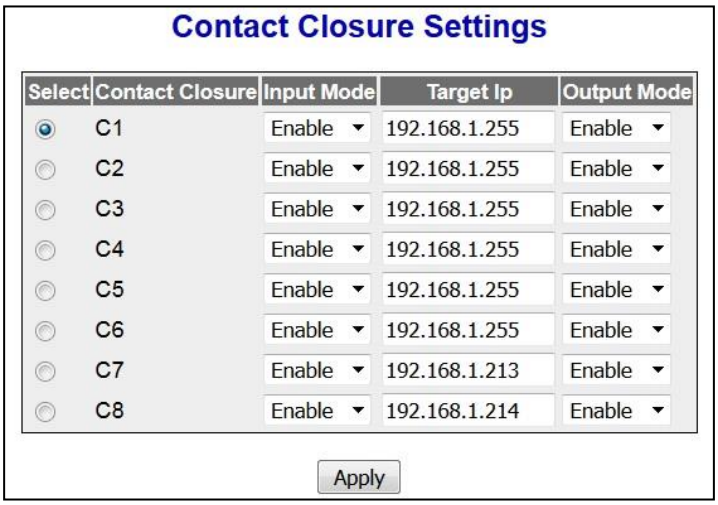


Figure 29-18 : Contact Closure Settings M-SES 1

Contact Closure Settings M-SES A

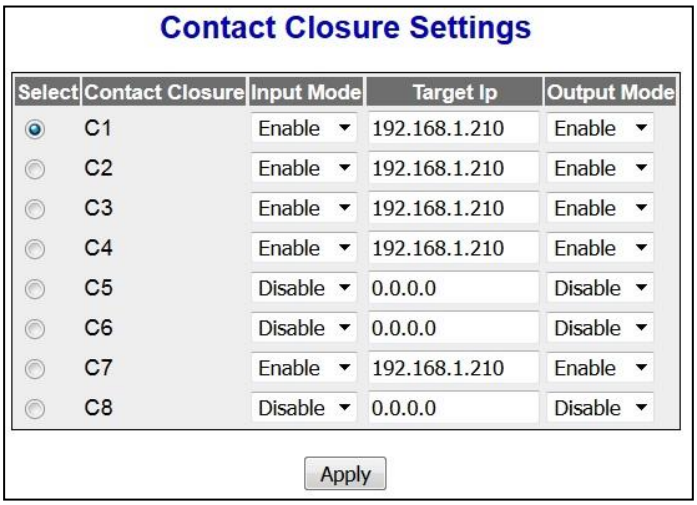


Figure 29-19 : Contact Closure Settings M-SES A

Contact Closure Settings M-SES B

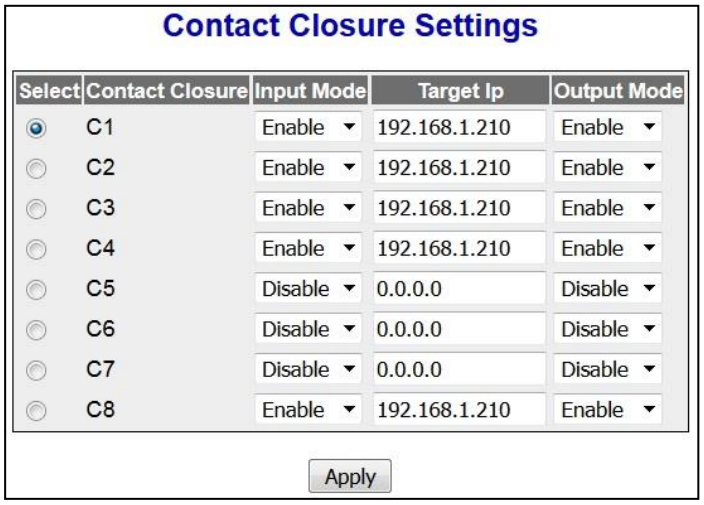


Figure 29-20 : Contact Closure Settings M-SES B

Contact Closure Settings M-SES C

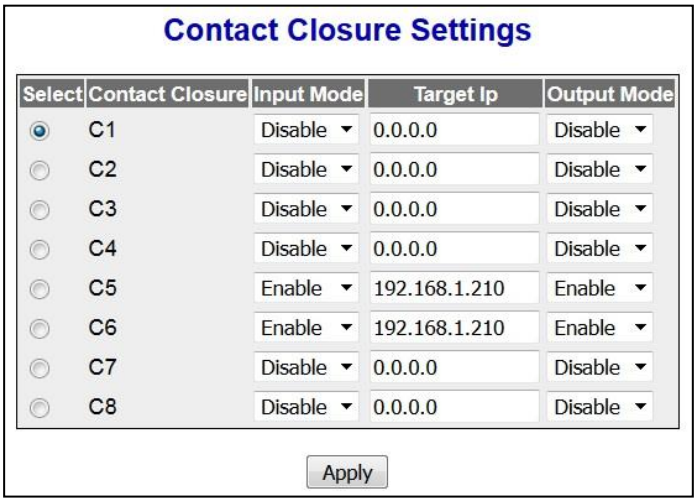


Figure 29-21 : Contact Closure Settings M-SES C

Contact Closure Settings M-SES D

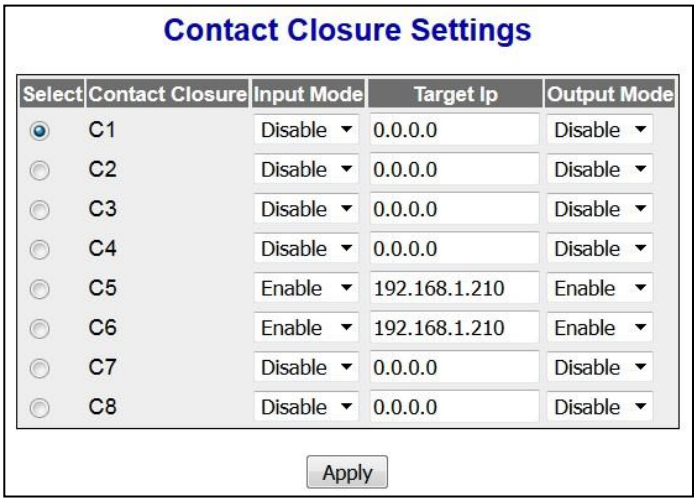


Figure 29-22 : Contact Closure Settings M-SES D

Chapter 29

High-Speed IO Ports

The high speed serial data over IP application can be used in several ways, but the use cases can be divided into three typical applications:

- Point-to-Point
- Point-to-Multipoint (typically a master-slave application)
- Multipoint-to-Point (unicast or broadcast)

Currently only point-to-point option is supported in M-SES software.

The High Speed IO parameters are configured through the screens displayed by the following tabs:

- High-Speed I/O
- High-Speed Serial Ports
- High-Speed Serial IP

To access Serial data I/O screens, click **I/O > HS-IO**

By default the tab **HS-IO** displays the **High-Speed I/O** screen.

30.1 HS-IO Global Configuration

In this way two serial devices can communicate over an IP network as two peers using UDP.

AMG 9IM2x/9HM2x web management interface supports configuring high speed serial port parameters such as serial port type, speed, number of data bits, number of stop bits etc.

Figure 30-1 : HS-IO Global configuration

☞ The Expander Module is connected to the M-SES unit by an external Ethernet (100Mbps) RJ45 to RJ45 Patch cable.

Screen Objective	This screen is used to enable global HS-IO port parameters for the serial ports on this device.
Navigation	**I/O > HS-IO > High-Speed I/O**
Fields	• **High Speed I/O Admin Mode** - to enable the mode for UDP/IP communication. If this field is not enabled, the switch will not transmit or receive any serial data related messages via UDP/IP to or from a remote device on the network. – **Enable** - enables the HS-IO – **Disable** - disables the HS-IO • **High Speed I/O Interface** - to select which Ethernet port on this device is used to connect to High-Speed I/O expander card. • **HS-I/O IP Address** - Use to assign a unique IP address to HS-I/O Expander. The IP address is not used to access HS-I/O device, but is used by the HS-I/O device to advertise gratuitous ARPs to any remote devices. This technique prevents serial data being flooded to all ports, so the destination is reached directly through MAC Address learning. •
Buttons	• Apply - button to apply configured changes to device.

30.2 HS-IO Serial Ports Configuration

The following web page shows 4 channels of data. The example below shows all 4x data channels being used to a number of IP targets.

Use this page to configure data transfer from Serial Channels (1-4) on this device to serial channels on remote devices.

Please use the switch below data connector on device in order to set serial channel type : RS-232 or RS-485 or RS-422.

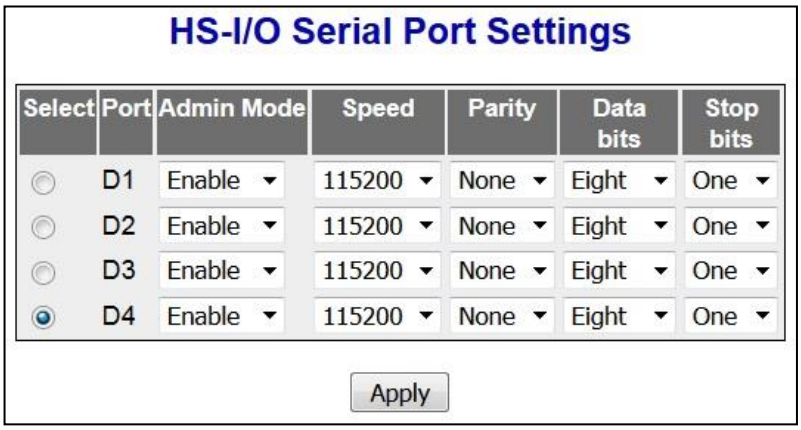


Figure 30-2 : HS-IO Serial Port Settings

Screen Objective	This screen is used to configure the individual HS-IO serial data port parameters on this device.
Navigation	**I/O > HS-IO > High-Speed Serial Ports**
Fields	• **Select** - the serial port to configure • **Port** - the serial port name • **Admin Mode** - to enable the serial port for UDP/IP communication. If this field is not enabled, the switch will not transmit or receive any serial data related messages via UDP/IP to or from the remote device on the network. – **Enable** - enables the serial port – **Disable** - disables the serial port • **Speed** - Baud rate at which serial port is to be operated. • **Parity bits** - parity bits in each character transferred over serial port. • **Data bits** - the number of data bits in each character transferred over serial port. • **Stop bits** - number of stop bits to be sent in each character transferred over serial port.

Buttons	• Apply - button to apply configured changes to device.

30.3 HS-IO Serial I/P Configuration

Use this page to configure data transfer from Serial Channels (1-4) on this device to serial channels on remote devices.

The following web page shows 4 channels of data. The example below shows all 4x data channels being used each with 2x IP address targets.

NOTE : It can take approximately 2 minutes per channel for the updated configuration to take effect when all 20 target IP addresses are configured per channel. So cumulatively it can take approximately 8 minutes for the whole configuration to take effect if all four channels are enabled and configured with 20 target IP addresses.

HS-I/O Serial IP Settings

Select	Target Ip Index	D1	D2	D3	D4
◉	1	192.168.1.210	192.168.1.210	192.168.1.210	192.168.1.210
○	2	192.168.1.211	192.168.1.212	192.168.1.213	192.168.1.214
○	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	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
○	10	0.0.0.0	0.0.0.0	0.0.0.0	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
○	13	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
○	14	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
○	15	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
○	16	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
○	17	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
○	18	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
○	19	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
○	20	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Apply

Figure 30-3 : HS-IO Serial Port Settings

Screen Objective	This screen is used to configure the individual HS-IO serial data IP parameters on this device.
Navigation	**I/O > HS-IO > High-Speed Serial IP**
Fields	• **Select** - the target IP / serial ports to configure • **Target IP Index (1-20)** - An index used for up to 4x 20 IP addresses. IP address of M-SES unit to which you wish to send serial data traffic. If more than one IP address is configured, then serial data will be sent to each target IP address. • **D1** - Target IP address for HS serial data port D1 • **D2** - Target IP address for HS serial data port D2 • **D3** - Target IP address for HS serial data port D3 • **D4** - Target IP address for HS serial data port D4
Buttons	• Apply - button to apply configured changes to device.

Chapter 30

Interface Statistics

The **Interface** link allows the user to view the interface related statistics screens through the following tabs**.**

- Interface Clear
- Interface
- Ethernet

By default, the tab **Interface Clear** displays the **Clear Interface Statistics** screen.

31.1 Clear Interface Statistics

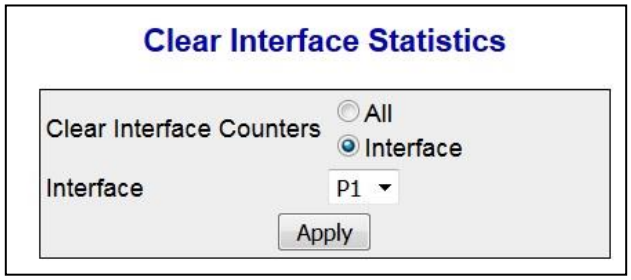
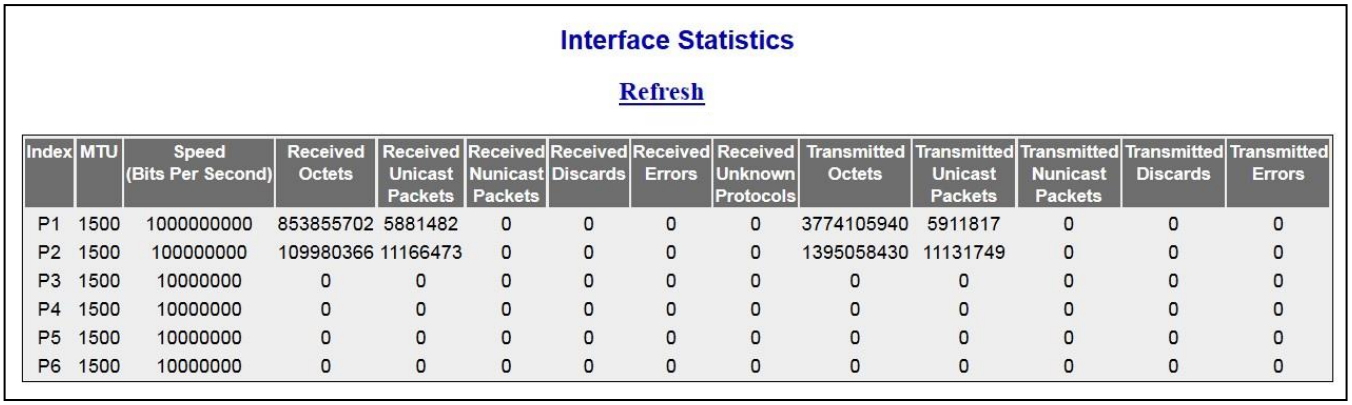


Figure 31-1 : Clear Interface Statistics

Screen Objective	This screen allows the user to clear the details in the interface counter for a particular interface or for all the interfaces.
Navigation	**Statistics > Interface > Interface Clear**

31.2 Interface Statistics



Interface Statistics

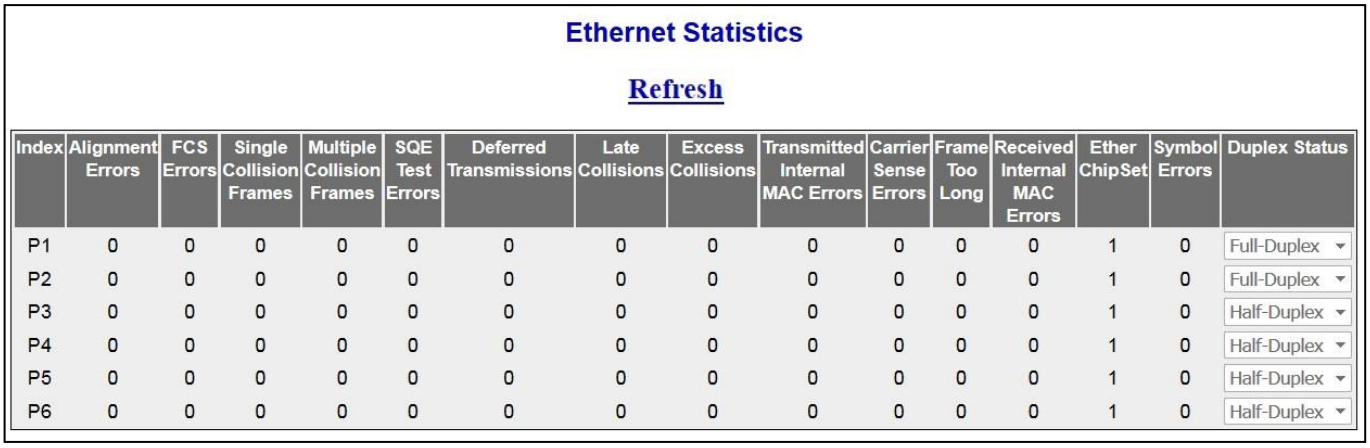
Refresh

Index	MTU	Speed (Bits Per Second)	Received Octets	Received Unicast Packets	Received Nunicast Packets	Received Discards	Received Errors	Received Unknown Protocols	Transmitted Octets	Transmitted Unicast Packets	Transmitted Nunicast Packets	Transmitted Discards	Transmitted Errors
P1	1500	1000000000	853855702	5881482	0	0	0	0	3774105940	5911817	0	0	0
P2	1500	100000000	109980366	11166473	0	0	0	0	1395058430	11131749	0	0	0
P3	1500	10000000	0	0	0	0	0	0	0	0	0	0	0
P4	1500	10000000	0	0	0	0	0	0	0	0	0	0	0
P5	1500	10000000	0	0	0	0	0	0	0	0	0	0	0
P6	1500	10000000	0	0	0	0	0	0	0	0	0	0	0

Figure 31-2 : Interface Statistics

Screen Objective	This screen displays the management information applicable to all the interfaces available in the Switch.
Navigation	**Statistics > Interface > Interface**

31.3 Ethernet Statistics



Ethernet Statistics

Refresh

Index	Alignment Errors	FCS Errors	Single Collision Frames	Multiple Collision Frames	SQE Test Errors	Deferred Transmissions	Late Collisions	Excess Collisions	Transmitted Internal MAC Errors	Carrier Sense Errors	Frame Too Long	Received Internal MAC Errors	Ether ChipSet	Symbol Errors	Duplex Status
P1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Full-Duplex
P2	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Full-Duplex
P3	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex
P4	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex
P5	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex
P6	0	0	0	0	0	0	0	0	0	0	0	0	1	0	Half-Duplex

Figure 31-3 : Ethernet Statistics

Screen Objective	This screen displays the statistics for a collection of Ethernet-like interfaces attached to the M-SES.
Navigation	**Statistics > Interface > Ethernet**

Chapter 31

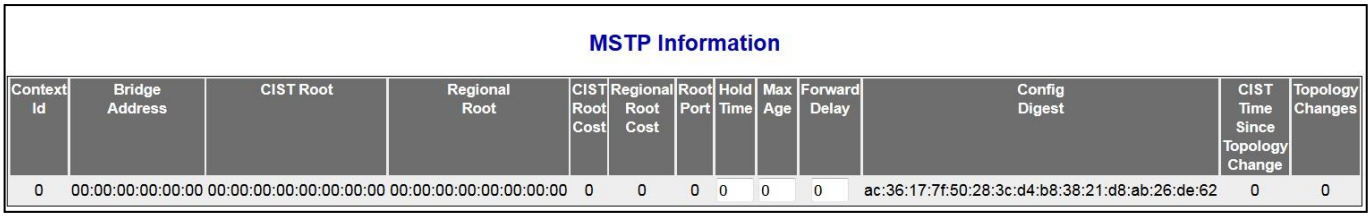
MSTP Statistics

The **MSTP** link allows the user to view the MSTP statistics screens through the following tabs.

- MSTP Information
- CIST Port Statistics
- MSTI Port Statistics

By default, the tab **MSTP Information** displays the **MSTP Information** screen.

32.1 MSTP Information



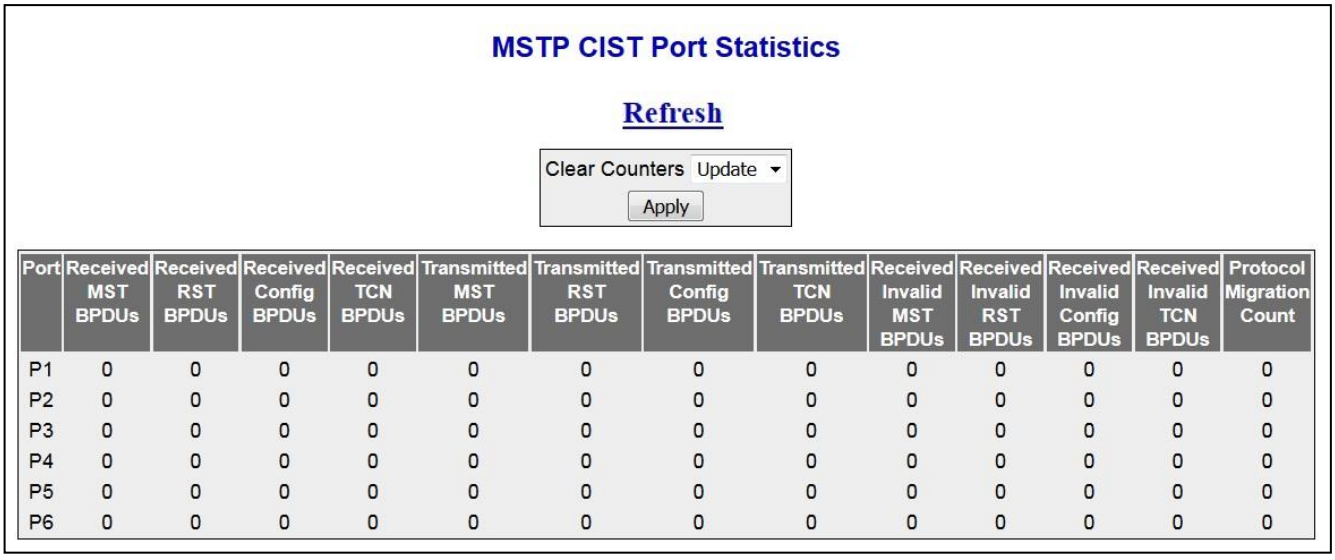
MSTP Information

Context Id	Bridge Address	CIST Root	Regional Root	CIST Root Cost	Regional Root Cost	Root Port	Hold Time	Max Age	Forward Delay	Config Digest	CIST Time Since Topology Change	Topology Changes
0	00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	0	0	0	0	0	0	ac:36:17:7f:50:28:3c:d4:b8:38:21:d8:ab:26:de:62	0	0

Figure 32-1 : MSTP Information

Screen Objective	This screen the information corresponding to the Multiple Spanning Tree protocol.
Navigation	**Statistics > MSTP > MSTP Information**

32.2 MSTP CIST Port Statistics



MSTP CIST Port Statistics

Refresh

Clear Counters Update

Apply

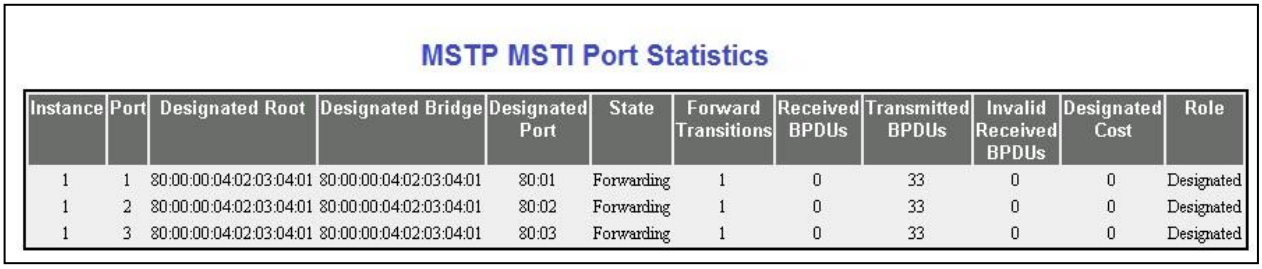
Port	Received MST BPDUs	Received RST BPDUs	Received Config BPDUs	Received TCN BPDUs	Transmitted MST BPDUs	Transmitted RST BPDUs	Transmitted Config BPDUs	Transmitted TCN BPDUs	Received Invalid MST BPDUs	Received Invalid RST BPDUs	Received Invalid Config BPDUs	Received Invalid TCN BPDUs	Protocol Migration Count
P1	0	0	0	0	0	0	0	0	0	0	0	0	0
P2	0	0	0	0	0	0	0	0	0	0	0	0	0
P3	0	0	0	0	0	0	0	0	0	0	0	0	0
P4	0	0	0	0	0	0	0	0	0	0	0	0	0
P5	0	0	0	0	0	0	0	0	0	0	0	0	0
P6	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 32-2 : MSTP CIST Port Statistics

Screen Objective	This screen displays the various MSTP statistics involved with each of the port available in the system
☞	The parameters in the screen are not populated with the values (the screen is blank), if the MSTP **System Control** status is set as Shutdown for the context selected using the **Context Selection** screen.
Navigation	**Statistics > MSTP > MSTP CIST Port Statistics**

Fields	**Clear Counters** - Select the option to update or clear the statistics for the interfaces on which MSTP is enabled.
Buttons	**Apply** - To select the required entry to clear the counters.

32.3 MSTP MSTI Port Statistics



MSTP MSTI Port Statistics

Instance	Port	Designated Root	Designated Bridge	Designated Port	State	Forward Transitions	Received BPDUs	Transmitted BPDUs	Invalid Received BPDUs	Designated Cost	Role
1	1	80:00:00:04:02:03:04:01	80:00:00:04:02:03:04:01	80:01	Forwarding	1	0	33	0	0	Designated
1	2	80:00:00:04:02:03:04:01	80:00:00:04:02:03:04:01	80:02	Forwarding	1	0	33	0	0	Designated
1	3	80:00:00:04:02:03:04:01	80:00:00:04:02:03:04:01	80:03	Forwarding	1	0	33	0	0	Designated

Figure 32-3 : MSTP MSTI Port Statistics

Screen Objective	This screen displays the statistics for the MSTI Ports in the system.
☞	This screen displays statistics only if, • MSTP **System Control** status is set as Start for the context selected using the **Context Selection** screen. • MSTI Instance is created using is created using the **VLAN Mapping** screen
Navigation	**Statistics > MSTP > MSTI Port Statistics**

Chapter 32

RSTP Statistics

The **RSTP** link allows the user to view the RSTP statistics screens through the following tabs.

- Information
- Port Statistics

By default, the tab **Information** displays the **RSTP Information** screen.

33.1 RSTP Information

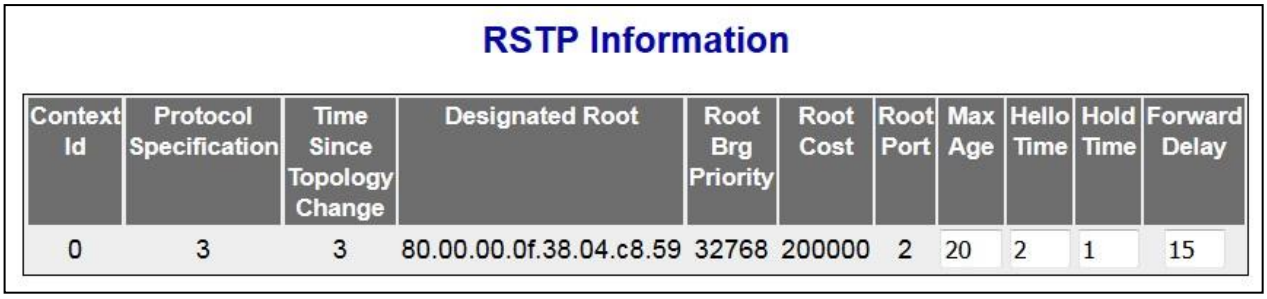


Figure 33-1 : RSTP Information

Screen Objective	This screen displays the RSTP information on the bridges that supports the Spanning Tree protocol.
☞	This screen displays the configuration details only for the context for which the RSTP **System Control** status is set as **Start**
Navigation	**Statistics > RSTP > Information**

33.2 RSTP Port Statistics

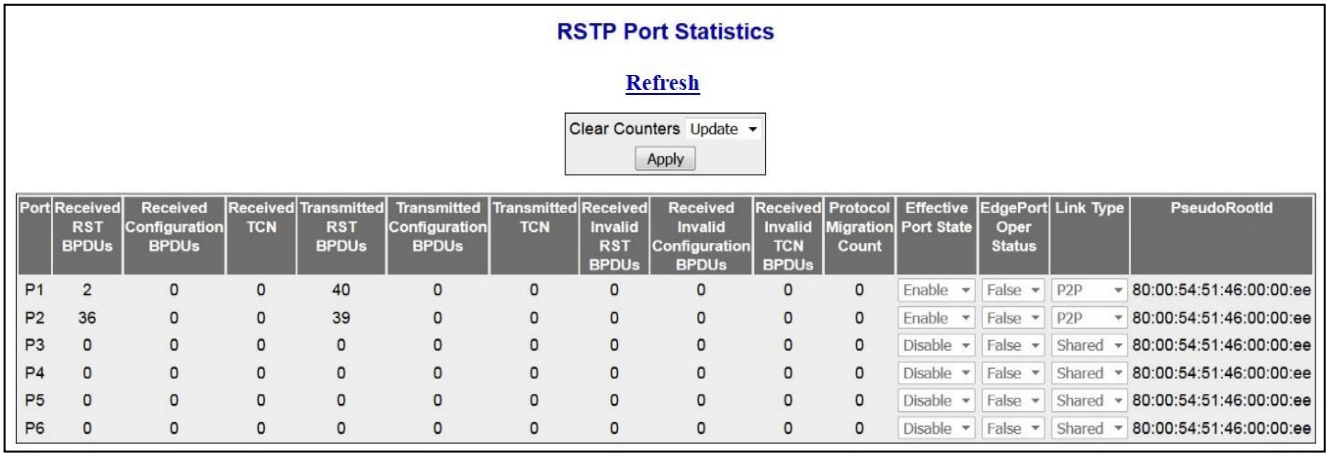


Figure 33-2 : RSTP Port Statistics

Screen Objective	This screen displays the various RSTP statistics involved with each of the port available in the system like the role, state, transition state machine, various packet statistics etc.

☞	The parameters in the screen are not populated with the values (the screen is blank), if the RSTP **System Control** status is set as Shutdown for the context selected using the **Context Selection** screen.
Navigation	**Statistics > RSTP > Port Statistics**
Fields	**Clear Counters** - Select the option to update or clear the statistics for the interfaces on which RSTP is enabled.
Buttons	**Apply** - To select the required entry to clear the counters.

Chapter 33

LLDP Statistics

The **LLDP** link allows the user to view the LLDP statistics screens through the following tabs**.**

- Traffic
- Statistics
- Errors

By default, the tab **Traffic** displays the **Traffic Information** screen.

34.1 LLDP Traffic Information

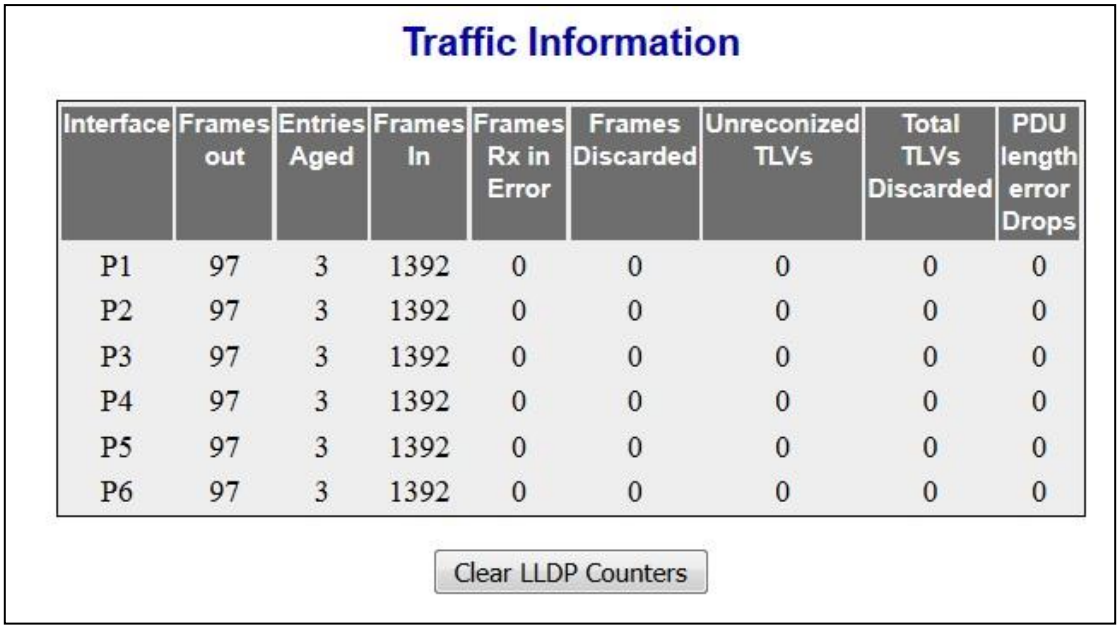


Figure 34-1 : LLDP Traffic Information

Screen Objective	This screen allows the user to view or clear the LLDP counters on specified interface. This includes the following for each interface: • Total Frames Out • Total Entries Aged • Total Frames In • Total Frames Received In Error • Total Frames Discarded • Total TLVS Unrecognized • Total TLVs Discarded • PDU Length error drops
Navigation	**Statistics > LLDP >Traffic**
Buttons	**Clear LLDP Counters** - To clear the LLDP counters on all interfaces

34.2 LLDP Statistics Information

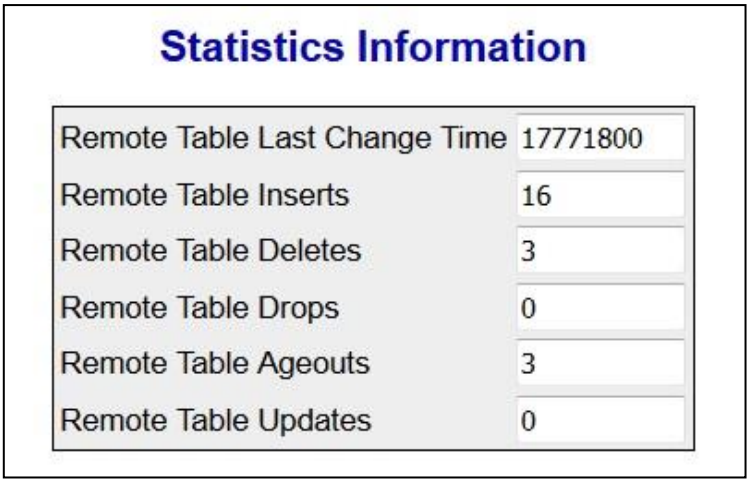


Figure 34-2 : LLDP Statistics Information

Screen Objective	This screen displays the LLDP remote table statistics information.
Navigation	**Statistics > LLDP >Statistics**

34.3 LLDP Error Information

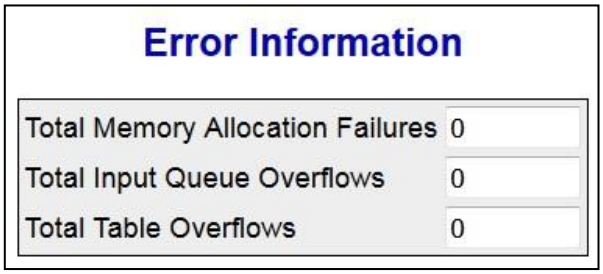


Figure 34-3 : LLDP Error Information

Screen Objective	This screen displays the details of LLDP error information such as total memory allocation failures and count of total input queue overflows.
Navigation	**Statistics > LLDP >Errors**

Chapter 34

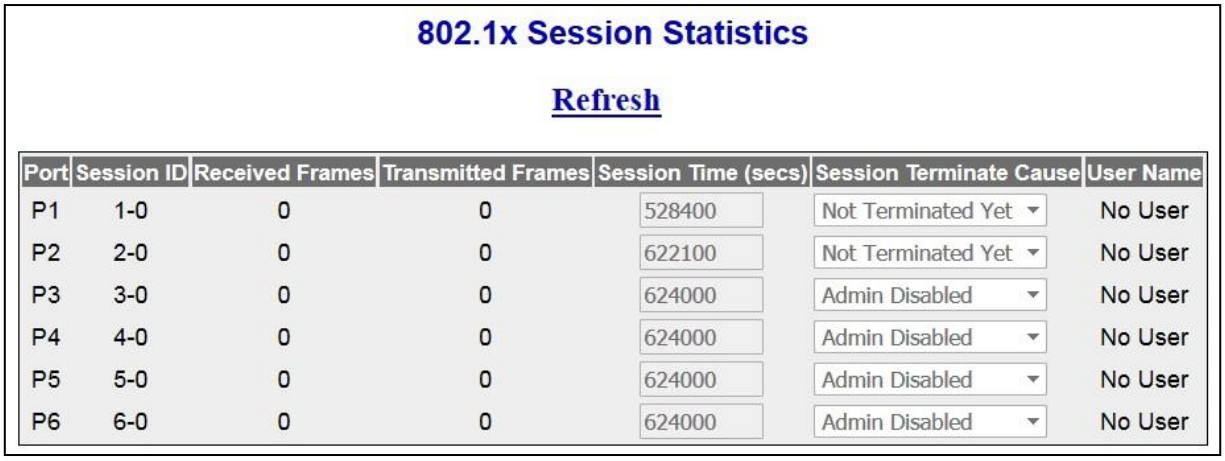
802.1x Statistics

The **802.1x** link allows the user to view the 802.1x statistics screens through the following tabs**.**

- Session Stats
- Supp Session Stats
- Mac Session Stats

By default, the tab **Session Stats** displays the **802.1x Session Statistics** screen.

35.1 802.1x Session Statistics



802.1x Session Statistics

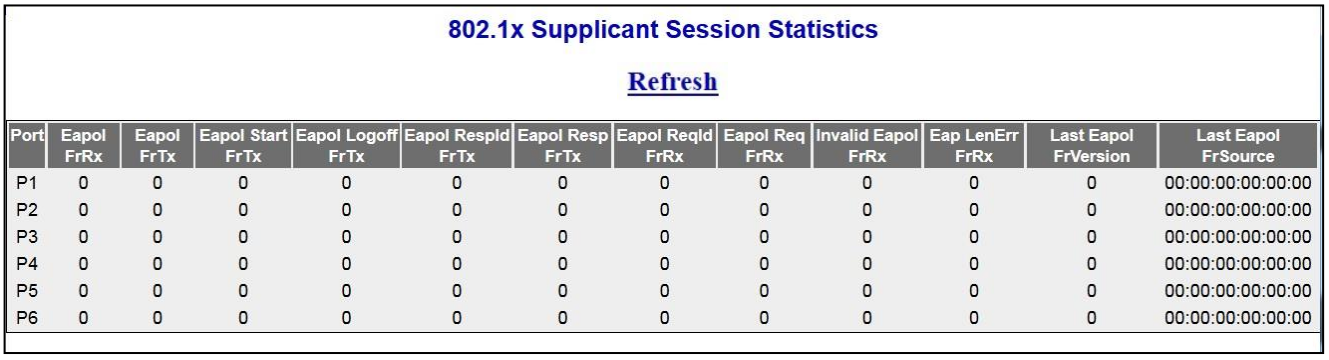
Refresh

Port	Session ID	Received Frames	Transmitted Frames	Session Time (secs)	Session Terminate Cause	User Name
P1	1-0	0	0	528400	Not Terminated Yet	No User
P2	2-0	0	0	622100	Not Terminated Yet	No User
P3	3-0	0	0	624000	Admin Disabled	No User
P4	4-0	0	0	624000	Admin Disabled	No User
P5	5-0	0	0	624000	Admin Disabled	No User
P6	6-0	0	0	624000	Admin Disabled	No User

Figure 35-1 : 802.1x Session Statistics

Screen Objective	This screen displays the session statistics for an authenticator PAE (Port Access Entity). It shows the current values collected for each session that is still in progress or the final values for the last valid session on each port where there is no current active session.
Navigation	**Statistics > 802.1x > Session Stats**

35.2 802.1x Supplicant Session Statistics



802.1x Supplicant Session Statistics

Refresh

Port	Eapol FrRx	Eapol FrTx	Eapol Start FrTx	Eapol Logoff FrTx	Eapol RespId FrTx	Eapol Resp FrTx	Eapol ReqId FrRx	Eapol Req FrRx	Invalid Eapol FrRx	Eap LenErr FrRx	Last Eapol FrVersion	Last Eapol FrSource
P1	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
P2	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
P3	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
P4	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
P5	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
P6	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00

Figure 35-2 : 802.1x Supplicant Session Statistics

Screen Objective	This screen displays the Supplicant Session statistics.
Navigation	**Statistics > 802.1x > Supp Session Stats**

35.3 802.1x MAC Session Statistics

Figure 35-3 : 802.1x MAC Session Statistics

Screen Objective	This screen displays the MAC Session statistics.
Navigation	**Statistics > 802.1x > MAC Session Stats**

Chapter 35

Radius Server Statistics

Radius Server Statistics

Index	Radius Server Address	UDP Port Number	Round Trip Time	No of Request Packets	No of Retransmitted Packets	No of Access-Accept Packets	No of Access-Reject Packets	No of Access-Challenge Packets	No of Malformed Access Responses	No of Bad Authenticators	No of Pending Requests	No of Time Outs	No of Unknown Types
1	25.0.0.1	1	0	0	0	0	0	0	0	0	0	0	0

Figure 36-1 : Radius Server Statistics – Statistics Group

Screen Objective	This screen displays the RADIUS Server statistics.
Navigation	**Statistics > Radius**

Chapter 36

IGMP Snooping Statistics

The **IGMP Snooping** link allows the user to view the IGMP Snooping related statistics screens through the following tabs**.**

- IGS Clear Statistics
- IGS Statistics
- IGS Version 3 Statistics

By default, the tab **IGS Clear Statistics** displays the **IGMP Snooping Clear Statistics** screen.

37.1 IGMP Snooping Clear Statistics

Figure 37-1 : IGMP Snooping Clear Statistics

Screen Objective	This screen the IGMP snooping clear statistics.
Navigation	**Statistics > IGMP Snooping > IGS Clear Statistics**

37.2 IGMP Snooping V1/V2 Statistics

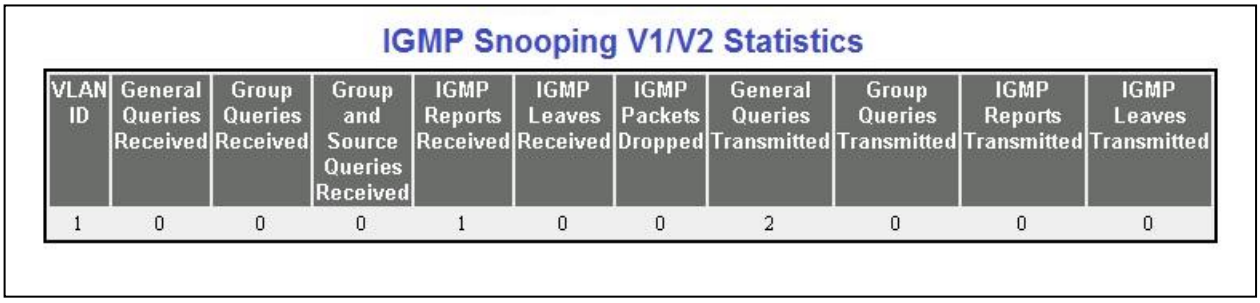


Figure 37-2 : IGMP Snooping V1/V2 Statistics

Screen Objective	This screen displays the IGMP snooping statistics pertaining to IGMP snooping v1 and v2.
Navigation	**Statistics > IGMP Snooping > IGS Statistics**

37.3 IGMP Snooping V3 Statistics

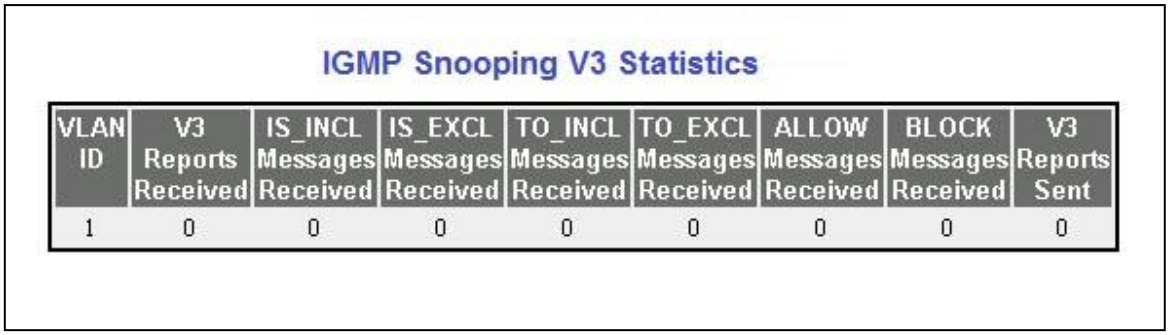


Figure 37-3 : IGMP Snooping V3 Statistics

Screen Objective	This screen displays the IGMP snooping statistics pertaining to IGMP snooping v3.
Navigation	**Statistics > IGMP Snooping > IGS Version 3 Statistics**

Chapter 37

IP Statistics

The **IP** link allows the user to view the IPv4 related statistics screens through the following tabs**.**

- ARP cache
- ICMP Statistics

By default, the tab **ARP Cache** displays the **ARP Cache** screen.

38.1 IPV4 ARP Cache Statistics

ARP Cache

Interface	MAC Address	IP Address	Media Type
vlan1	54:51:46:00:00:d0	192.168.0.102	Dynamic
vlan1	c8:0a:a9:89:d0:09	192.168.0.211	Dynamic
vlan1	34:64:a9:7c:95:a1	192.168.0.232	Dynamic

Figure 38-1 : IPV4 ARP Cache

Screen Objective	This screen displays the ARP cache related statistics information such as MAC address, for all interfaces of the switch.
Navigation	**Statistics > IP > ARP Cache**

38.2 IPV4 ICMP Statistics

ICMP Statistics

Received Message	1
Received Error	1
Receive Destination Unreachable	0
Received Redirect	0
Received Echo Requests	1
Received Echo Replies	0
Receive Source Quenches	0
Transmitted Message	251
Transmitted Error	0
Transmited Destination Unreachable	0
Transmitted Redirect	251
Transmitted Echo Requests	0
Transmitted Echo Replies	0
Transmited Source Quenches	0

Figure 38-2 : IPV4 ICMP Statistics

Screen Objective	This screen displays the ICMP transmission and reception related statistics information such as Received Redirect, Transmitted Error and so on.
Navigation	**Statistics > IP > ICMP Statistics**

Chapter 38

SNMP Statistics

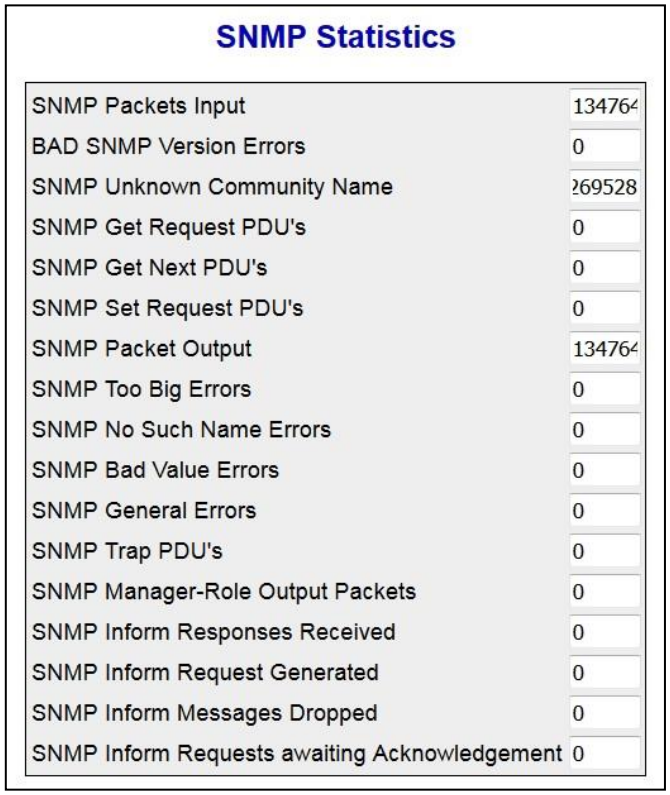


Figure 39-1 : SNMP Statistics

Screen Objective	This screen displays the statistics information related to SNMP Agent.
Navigation	**Statistics > SNMP**