VadaTech Managed Gigabit Ethernet Switch

VadaTech Gigabit Ethernet Switch Web Interface Reference Manual

February 8, 2010

Version 1.3

vadatech inc

THE POWER OF VISION

Copyright

Notice

While reasonable efforts have been made to assure the accuracy of this document, VadaTech, Inc. assumes no liability resulting from any omissions in this document or from the use of the information obtained herein. VadaTech reserves the right to revise this document and to make changes periodically and the content hereof without obligation of VadaTech to notify any person of such revision or changes.

Electronic versions of this material may be read online, downloaded for personal use, or referenced in another document as a URL to the VadaTech Incorporated Web site. The text itself may not be published commercially in print or electronic form, edited, translated, or otherwise altered without the permission of VadaTech, Inc.

It is possible that this publication may contain reference to or information about VadaTech products (machines and programs), programming, or services that are not available in your country. Such references or information must not be construed to mean that VadaTech intends to announce such products, programming, or services in your country.

Trademarks

The VadaTech, Inc name and logo are registered trademarks of VadaTech Incorporated in the U.S.A. All other product or service names mentioned in this document are the property of their respective owners.

Revision History

Doc Rev	Description of Change	Revision Date
1.0	Document Created	03/18/2009
1.1	Update to include ATC114, UTC002, UTC003 Include port based VLAN	09/17/2009
1.2	Update to include CP218 and AMC228	11/04/2009
1.3	Update to include VT851, VT852, VT853 and ATC809	02/08/2010

Table of Contents

Figures

Tables

1 Overview

Several VadaTech products contain Layer 2 managed switch functionality. The VadaTech Gigabit Ethernet Switch Web Interface is an embedded web-based management system which provides switch management features and basic Layer 2 protocols such as IEEE 802.1w rapid spanning tree, IEEE 802.1x port-based access control, and IGMP snooping.

1.1 Supported Products

- VadaTech UTC001 with L2 Managed Switch option (B=1)
- VadaTech UTC002 with L2 Managed Switch option (B=1)
- VadaTech UTC003 with L2 Managed Switch option (B=1)
- VadaTech VT850
- VadaTech VT851
- VadaTech VT852
- VadaTech VT853
- VadaTech AMC216
- VadaTech AMC217
- VadaTech AMC218
- VadaTech AMC219
- VadaTech AMC228
- VadaTech ATC114
- VadaTech ATC809
- VadaTech CP218

1.2 Document References

- PICMG® 3.0 Revision 3.0 AdvancedTCA® Base Specification
- PICMG® AMC.0 R2.0 Advanced Mezzanine Card Base Specification
- RFC 1112
- RFC 2236
- RFC 2865
- RFC 3164

1.3 Acronyms Used in this Document

Acronym	Description
AMC	Advanced Mezzanine Card
ARL	Address Resolution List
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol over LAN
FCS	Frame Check Sum
GbE	Gigabit Ethernet
IGMP	Internet Group Management Protocol
L2	Layer 2
MAC	Media Access Control
MCH	MicroTCA Carrier Hub
MGCP	Media Gateway Control Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RSTP	Rapid Spanning Tree Protocol
SCCP	Skinny Call Control Protocol
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
VID	VLAN Id
VLAN	Virtual Local Area Network
VoIP	Voice over IP

Table 1: Acronyms

2 Web-based Management Functions

2.1 Web Functions

The VadaTech Gigabit Ethernet Switch Web interface supports the Layer 2 features and protocols described in the following subsections.

Function	Short Description
System Level	System configuration
Port	Port configuration
Statistics	Statistical monitoring
VLAN	VLAN configuration
Trunking	Trunk Group configuration
Mirror	Mirror configuration
QoS	Quality of Service configuration
Rate	Rate Limit configuration
L2 Management	L2 Address Management
802.1x	Port Authentication configuration
IGMP Snooping	IGMP Snooping configuration
Auto DoS	Automatic Denial of Service Prevention
Auto VoIP	Automatic Voice over IP configuration
Logging	Logging configuration
Logout	Exit Management functions

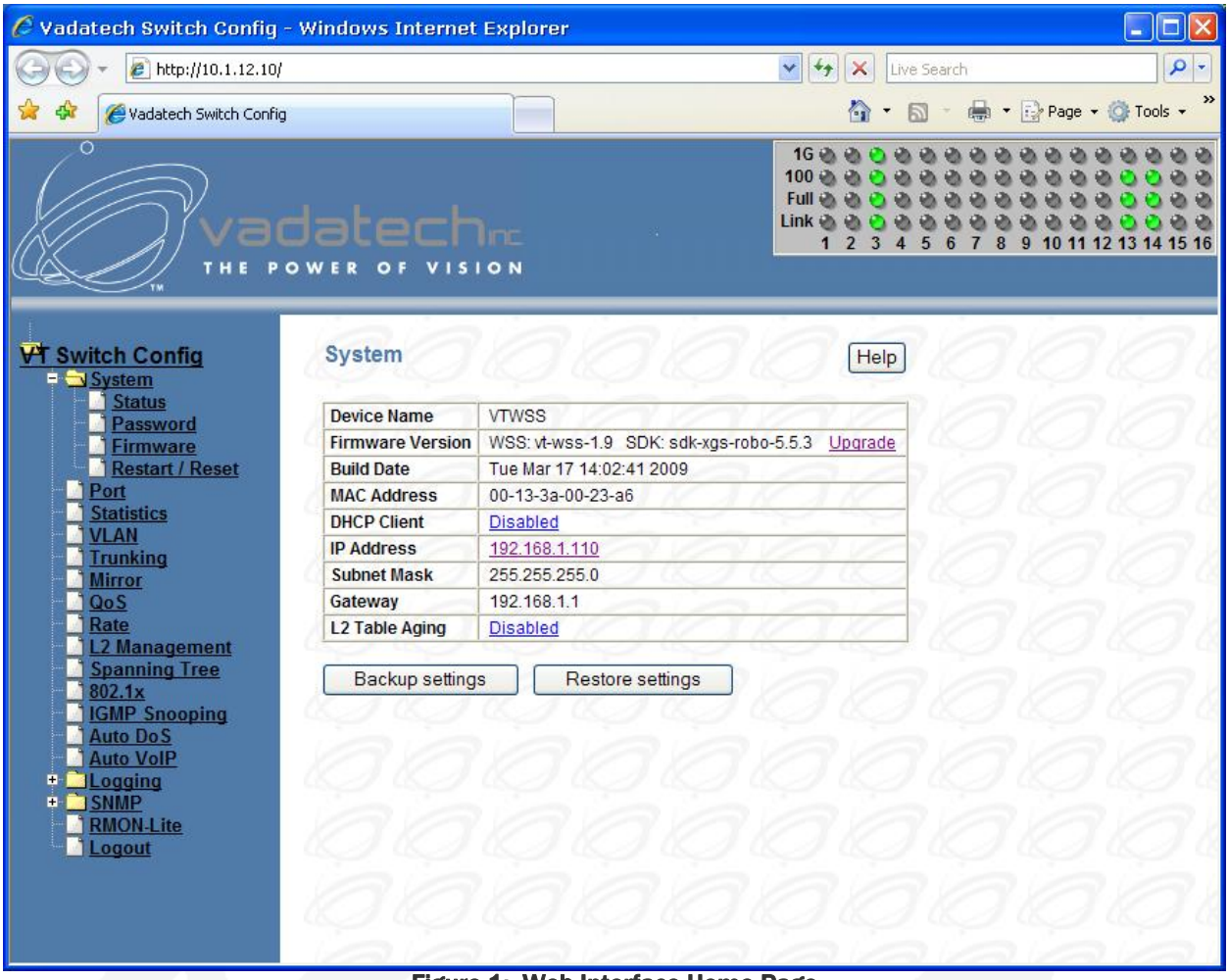


Figure 1: Web Interface Home Page

Note: All screen shots in this document are taken from the VadaTech UTC001. Other supported products may differ in the number of ports and connections supported.

2.1.1 System Level

The DHCP and static IP address are supported to assign the IP address of the device. The firmware upgrade, backup, and restore configuration data help to protect and upgrade the system. System password access allows administrative access to change password authentication. The system model number and revision are also supported.

2.1.2 Port

Port displays the status of all ports.

2.1.3 Statistics

The statistics function shows port counters from a top view and shows the details of breakdown counters, including good and bad frames. A Refresh button allows for the retrieval of the latest values of the counters.

2.1.4 VLAN

The VLAN function supports configuration, creation, or removal of IEEE 802.1Q VLANs with a specific VLAN ID. The range of the VLAN ID is 2 to 4094 (0 and 4095 are reserved, 1 is the default VLAN).

2.1.5 Trunking

This creates trunk groups and assigns member ports in the trunk. The member ports of the trunk are aggregated to enlarge the bandwidth. The distribution algorithm balances traffic-loading across the trunk.

2.1.6 Mirroring

The mirroring feature monitors traffic from the specified port to the mirror to port. Egress mirroring monitors outgoing traffic; ingress mirroring monitors incoming traffic.

2.1.7 QoS

This function supports IEEE 802.1P operation and allows for priority assignment to CoS queue mapping. Scheduling algorithms such as strict, round robin, and weighted round robin are supported.

2.1.8 Rate

Rate control determines the bandwidth from ingress or egress.

2.1.9 Spanning tree

The system supports IEEE 802.1w rapid spanning tree operation, which configures related parameters in the bridge base and the port base.

2.1.10 802.1x

The IEEE 802.1x protocol controls port-based access. Authentication parameters can be controlled from this function, and the authentication status of each port is displayed.

2.1.11 IGMP Snooping

This feature supports IGMP snooping to configure related parameters.

2.1.12 AutoDoS

This feature prevents an attack on a computer system or network that would otherwise cause a loss of service to users.

2.1.13 Auto VoIP

This feature provides a mechanism to classify VoIP Packets so that they can be prioritized above data packets in order to achieve better Quality of Service (QoS).

2.1.14 Logging

This feature is used to record various system messages and events.

2.1.15 Logout

Exits the Web Interface.

3 Web Interface Home Page

The VadaTech Gigabit Ethernet Switch Web Interface provides an embedded Web engine for configuration and management from a remote standard Web browser. The Web-based GUI home page appears in Error! Reference source not found..

There are three main areas in this page:

- The LED panel display shows the link status.
- The Command frame lists all supported features. Click on items in the command list to control a function.
- The Function frame displays function and management components.

3.1 System Information

The system information screen lists system settings as shown in Figure 2.

Figure 2: System Information

- **Firmware Version** displays the revision ID of the system. The Upgrade option initiates a Firmware upgrade.
- **MAC Address** indicates the MAC address of the out-of-band Ethernet interface.
- **Build Date** indicates the date the firmware was created.
- **DHCP Client** allows for enabling or disabling of the DHCP client. The IP address of the system is retrieved from the DHCP server during enabling, but the IP address cannot be set from this screen.
- **IP Address** indicates the IP address of the system.

- **Subnet Mask** is the subnet mask of the IP address.
- **Gateway** is the IP address of the gateway for the remote manager.
- **L2 Table Aging** defines the aging time of the ARL table. Select 0 to disable.

3.1.1 Backup Settings

Backup Settings allows the current system configuration to be saved and archived to an external host.

3.1.2 Restore Settings

Restore Settings helps to restore a previously backed-up system configuration file from an external host.

3.2 Port Function

3.2.1 Port Status

Port functions provide an overview of the system. The port status screen, shown in **Figure 3**, displays each port's status, such as link, speed, duplex, and flow control.

PORT Status

Refresh Help

Port	Name	Link Status	Speed Duplex	Flow Control	PVID	Port	Name	Link Status	Speed Duplex	Flow Control	PVID
1	AMC 1	Down	--	--	1	9	AMC 9	Down	--	--	1
2	AMC 2	Down	--	--	1	10	AMC 10	Down	--	--	1
3	AMC 3	Down	--	--	1	11	AMC 11	Down	--	--	1
4	AMC 4	Down	--	--	1	12	AMC 12	Down	--	--	1
5	AMC 5	Down	--	--	1	13	MCH Management	Up	100Mbps Full	Disabled	1
6	AMC 6	Down	--	--	1	14	Front Panel	Down	--	--	1
7	AMC 7	Down	--	--	1	15	MCH Expansion	Down	--	--	1
8	AMC 8	Down	--	--	1	16	MCH Update	Up	1000Mbps Full	Disabled	1

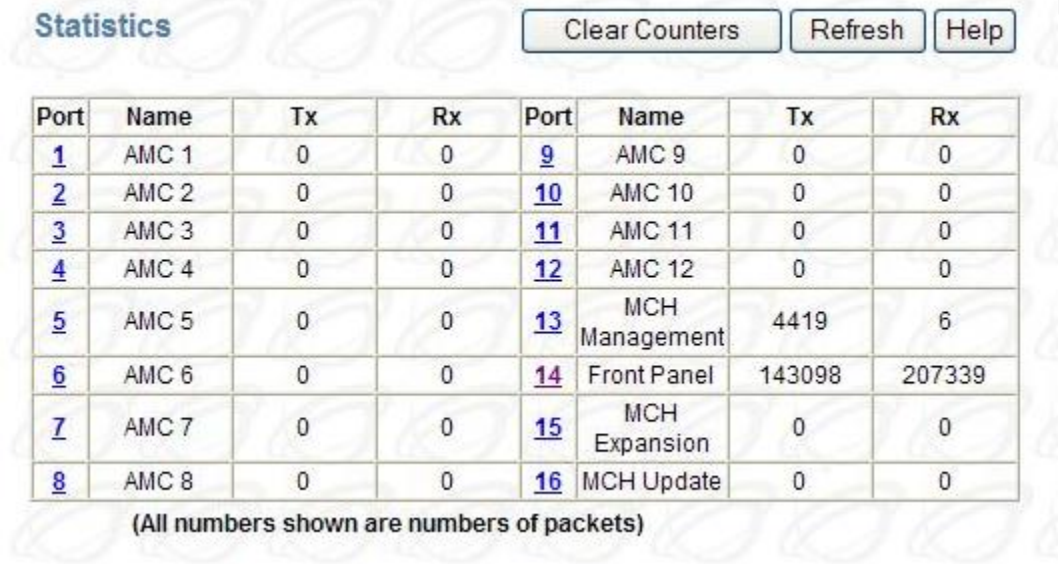
Figure 3: Port Status

- **Port** indicates the port numbers of the system.
- **Name** indicates the place the port is connected in the system.
- **Link Status** displays the link status of the port (up or down).
- **Speed Duplex** indicates the speed (10/100/1000 Mbps) and duplex (Half/Full) of the port when the links are up. If the link is down there is no display.
- **Flow Control** indicates the state of flow control if the port is linked up. It supports fair access to buffering resources while also enabling lossless operation across a network of Ethernet switching devices.
- **PVID** indicates the VLAN id that untagged packets entering the switch through the associated port will use.
- The **Refresh** button updates the display with the current status.

3.3 Statistics

3.3.1 Statistics Overview

The statistics screen display traffic counters for each port as shown in **Figure 4:** Statistics Overview.



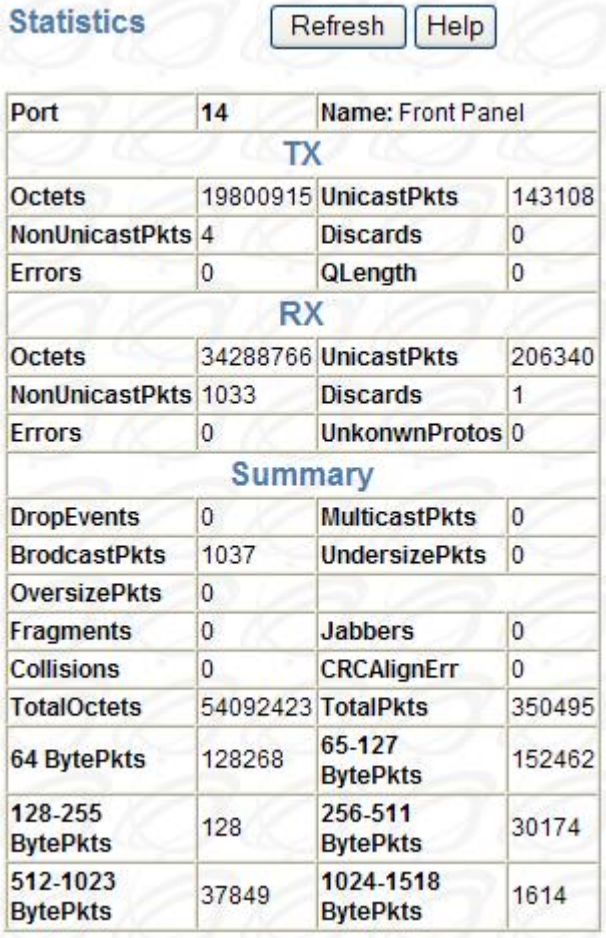
Port	Name	Tx	Rx	Port	Name	Tx	Rx
1	AMC 1	0	0	9	AMC 9	0	0
2	AMC 2	0	0	10	AMC 10	0	0
3	AMC 3	0	0	11	AMC 11	0	0
4	AMC 4	0	0	12	AMC 12	0	0
5	AMC 5	0	0	13	MCH Management	4419	6
6	AMC 6	0	0	14	Front Panel	143098	207339
7	AMC 7	0	0	15	MCH Expansion	0	0
8	AMC 8	0	0	16	MCH Update	0	0

Figure 4: Statistics Overview

- **Tx** indicates the total packets transmitted from the port.
- **Rx** indicates the total packets received by the ports.
- The **Clear Counters** button resets the packet counts for all ports to zero.
- The **Refresh** button updates the display with the current statistics.

3.3.2 Port Statistics

The port statistics screen displays traffic counters for each port as shown in Figure 5.



Statistics Refresh Help

Port	14	Name: Front Panel	
TX			
Octets	19800915	UnicastPkts	143108
NonUnicastPkts	4	Discards	0
Errors	0	QLength	0
RX			
Octets	34288766	UnicastPkts	206340
NonUnicastPkts	1033	Discards	1
Errors	0	UnkonwnProtos	0
Summary			
DropEvents	0	MulticastPkts	0
BrodcastPkts	1037	UndersizePkts	0
OversizePkts	0		
Fragments	0	Jabbers	0
Collisions	0	CRCAlignErr	0
TotalOctets	54092423	TotalPkts	350495
64 BytePkts	128268	65-127 BytePkts	152462
128-255 BytePkts	128	256-511 BytePkts	30174
512-1023 BytePkts	37849	1024-1518 BytePkts	1614

Figure 5: Port Statistics

- TX
  - **Octets** indicates the total number of octets transmitted.
  - **UnicastPkts** indicates the number of transmitted unicast packets.
  - **NonUnicastPkts** indicates the number of transmitted nonunicast packets.
  - **Discards** indicates the number of discarded packets.
  - **Errors** indicates excessive collision packets.
  - **QLength** indicates the count of packets currently buffered.
- RX
  - **Octets** indicates the total number of octets received.
  - **UnicastPkts** indicates the number of received unicast packets.
  - **NonUnicastPkts** indicates the number of received nonunicast packets.
  - **Discards** indicates the number of discarded packets.
  - **Errors** indicates undersize/fragment/FCS error/oversized with good FCS packets.
  - **UnknownProtos** indicates received packets using unknown protocols.

- Summary
  - **DropEvents** indicates which are dropped do to GBP or backpressure discard packets.
  - **MulticastPkts** indicates transmitted/received multicast packets.
  - **BroadcastPkts** indicates transmitted/received broadcast packets.
  - **UndersizePkts** indicates received packets with length less than minimum packet size.
  - **OversizePkts** indicates received packets with length more than maximum packet size.
  - **Fragments** indicates received packets (length 10-63 bytes) with invalid FCS or alignment error.
  - **Jabbers** indicates received packets (invalid FCS or code error) which exceed counter maximum size to maximum receive frame length.
  - **Collisions** indicates total transmitted collision packets.
  - **CRCAlignErr** indicates received packets (invalid FCS) which length are between 64 bytes to maximum size.
  - **TotalOctets** indicates total received packets (excluding framing bits. but including FCS) and transmitted (including fragments of frames that were involved with collisions, but excluding preamble/SFD or jam bites) byte.
  - **TotalPkts** indicates total received and transmitted packet count (including bad packets, all unicast, broadcast, multicast and MAC control packets).
  - **64 BytePkts** indicates transmitted packets with packet length less than or equal to 64 bytes.
  - **65-127 BytePkts** indicates transmitted packets with packet length between 65 to 127 bytes, inclusive.
  - **128-255 BytePkts** indicates transmitted packets with packet length between 128 to 255 bytes, inclusive.
  - **256-511 BytePkts** indicates transmitted packets with packet length between 256 to 511 bytes, inclusive.
  - **512-1023 BytePkts** indicates transmitted packets with packet length between 512 to 1023 bytes, inclusive.
  - **1024-1522 BytePkts** indicates transmitted packets with packet length between 1024 to 1522 bytes, inclusive.
- The **Refresh** button updates the display with the current statistics.

3.4 VLAN

The VLAN function allows for the control of IEEE 802.1Q VLANs in the system. It supports the creation of a new VLAN, addition or removal of VLAN member ports, and removal of a VLAN from the system. VLANS with VID = 0 and 4095 are reserved. The VLAN with VID = 1 is the default VLAN, and it cannot be removed.

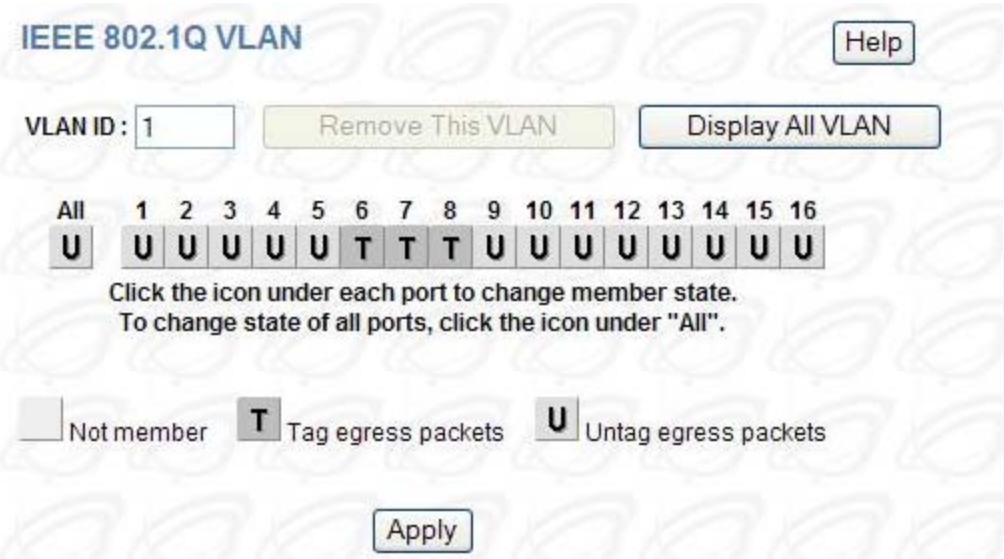


Figure 6: VLAN Port Membership

- **VLAN ID** indicates the VLAN ID to control.
- **Member Ports** indicates the number of the ports included in the VLAN. There are three symbols for each port.
  - *Empty* indicates that the port is not a member of the VLAN.
  - *U* indicates that this port is a member of the VLAN. When a packet leaves the member port, the VLAN tag is removed.
  - *T* indicates that this port is a member of the VLAN. When a packet leaves the member port, the VLAN tag is added.
- The **Remove This VLAN** button removes the VLAN from the system.
- The **Apply** button creates the VLAN and updates its member ports.
- The **Display All VLAN** button shows a list of all VLANs defined in the switch.

3.5 Trunking

Trunking allows multiple ports to be aggregated into a single trunk. It uses a distribution algorithm to balance traffic between trunk members. This aggregates the bandwidth of the trunk.

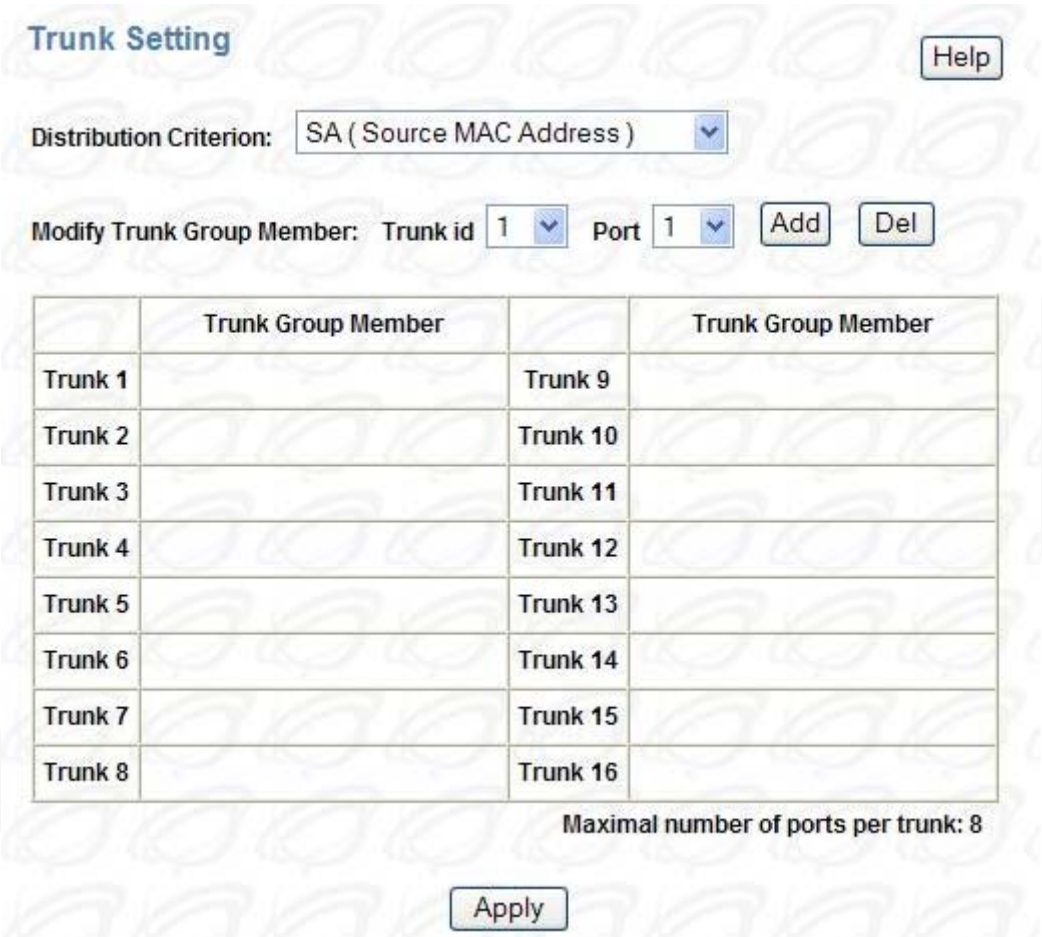


Figure 7: Trunk Setting

- **Distribution Criterion** defines the traffic distribution algorithm between trunk member ports.
- **Trunk Group** is the trunk group ID supported in this device.
- **Member Ports** defines member ports of the trunk.

3.6 Port Mirroring

Port mirroring monitors traffic from specific ports to a single mirror-to port. Ingress and/or egress traffic is copied from the mirroring port to the mirror-to port.

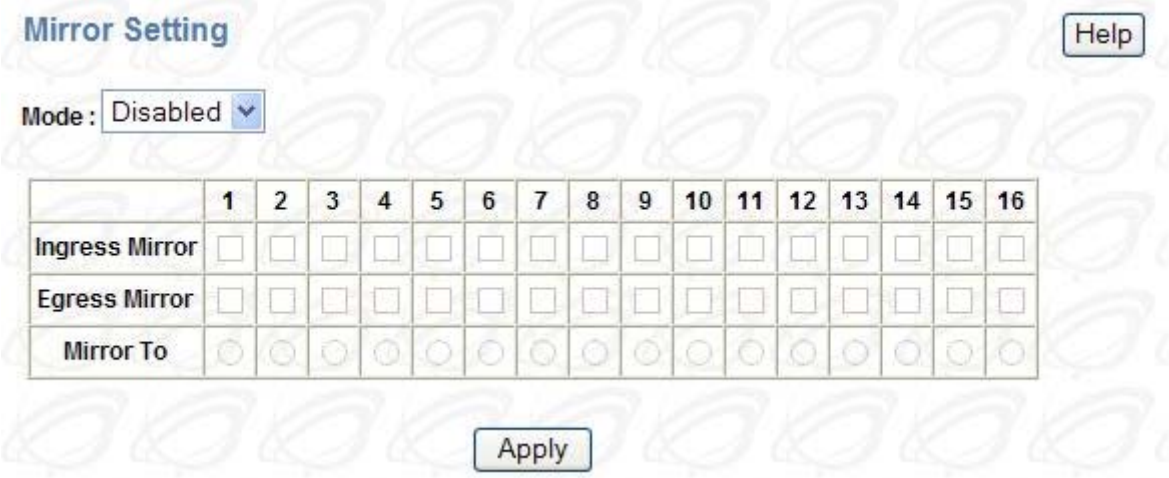


Figure 8: Mirror Setting

- Mode enables or disables mirroring.
- Ingress Mirror specifies an ingress mirror port to which ingress traffic is mirrored.
- Egress Mirror specifies an egress mirror port to which egress traffic is mirrored.
- Mirror To specifies the mirror-to port.

3.7 QoS

The QoS Setting screen sets the priority relationships between four queues, selects the scheduling method for these queues, associates packets of specific priorities to a specific queue, and specifies a weight for each queue.

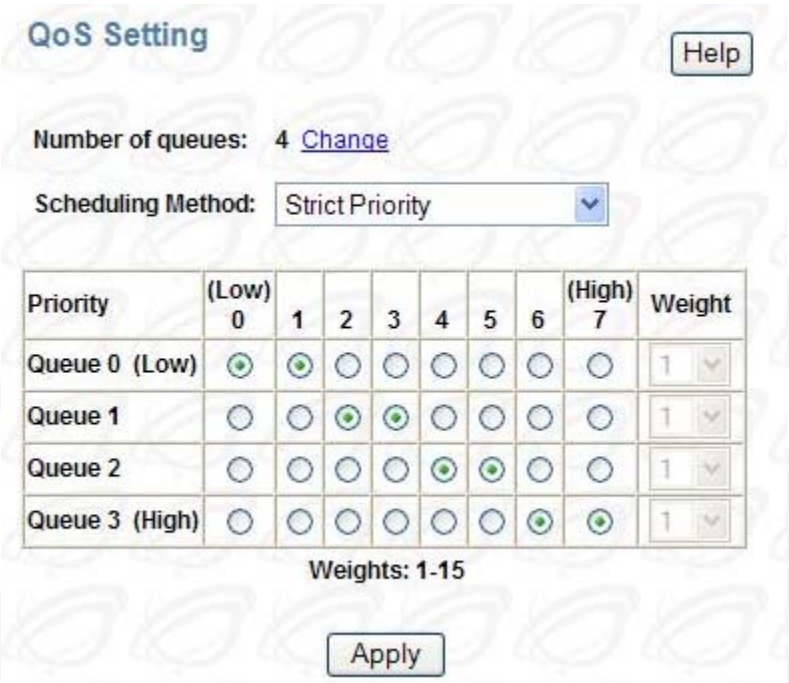


Figure 9: QoS Setting

- **Scheduling Method** specifies one of the two scheduling methods for the queues.
  - *Strict Priority* – This method biases the queuing mechanism to favor the higher queues over the lower queues. For example, strict priority queuing processes as many packets as possible in queue 3 before processing any packets from queue 2, then processes as many packets as possible in queue 2 before processing any packets in queue 1 or queue 0.
  - *Weighted Round Robin* – A weighted fair queuing algorithm is used to rotate service among the four queues. The rotation is based on the specified weights assigned to each queue; the number of packets serviced during each visit to a queue depends on the specified percentages. This method converts the specified percentages into weights for the queues.
- **Queue 0-3** specifies the four queues. Queue 0 is the lowest priority queue; queue 3 is the highest priority queue. Packets in queue 3 are served more often than packets in queue 0.
- **Priority** indicates the packet priority. This value is retrieved from the priority tag field, with values from 0 to 7; 0 indicates the lowest priority; 7 indicates the highest priority. Click the options to send packets of a specified priority to a particular queue.

- **Weight** indicates the weight (number of packets) to be served in the queue before moving to serve the next queue. A high-priority queue should have a higher weight than a low-priority queue.

3.8 Rate Control

Rate control determines the bandwidth of ingress and egress traffic for a specified port.

3.8.1 Rate Limit Overview

Figure 10 displays the ingress and egress traffic rate control data for each port in the system.

Rate Limit and Storm Control

Help

Port	Name	Ingress Rate	Egress Rate	Port	Name	Ingress Rate	Egress Rate
1	AMC 1	No Limit	No Limit	9	AMC 9	No Limit	No Limit
2	AMC 2	No Limit	No Limit	10	AMC 10	No Limit	No Limit
3	AMC 3	No Limit	No Limit	11	AMC 11	No Limit	No Limit
4	AMC 4	No Limit	No Limit	12	AMC 12	No Limit	No Limit
5	AMC 5	No Limit	No Limit	13	MCH Management	No Limit	No Limit
6	AMC 6	No Limit	No Limit	14	Front Panel	No Limit	No Limit
7	AMC 7	No Limit	No Limit	15	MCH Expansion	No Limit	No Limit
8	AMC 8	No Limit	No Limit	16	MCH Update	No Limit	No Limit
Storm Control		disabled					

Figure 10: Rate Limit Overview

- **Port** indicates the port number. Select the port number to control ingress and egress rates for the port.
- **Name** indicates the place the port is connected in the system.
- **Ingress Rate** indicates the rate limitation of incoming traffic on this port.
- **Egress Rate** indicates the rate limitation of outgoing traffic on this port.

3.8.2 Port Rate Limit

Figure 11: Port Rate Limit

- **Ingress Rate** selects the rate for incoming traffic.
- **Egress Rate** selects the rate for outgoing traffic.

3.8.3 Storm Control

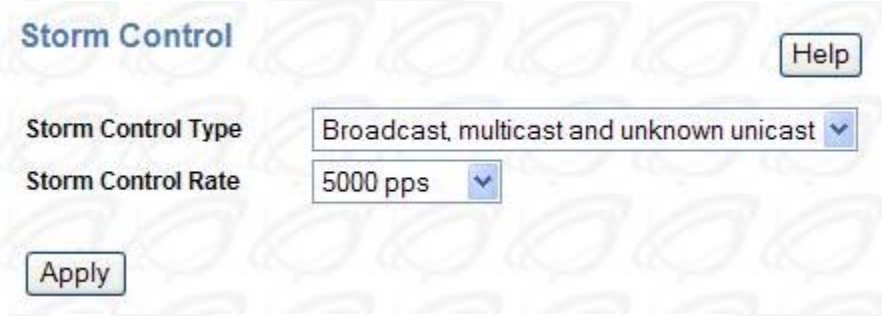


Figure 12: Storm Control

- **Storm Control Type** selects the type of the packet storm.
- **Storm Control Rate** selects the rate for storm control.

3.9 L2 Management

L2 address management provides a way to add, delete and lookup MAC address in the L2 address table.

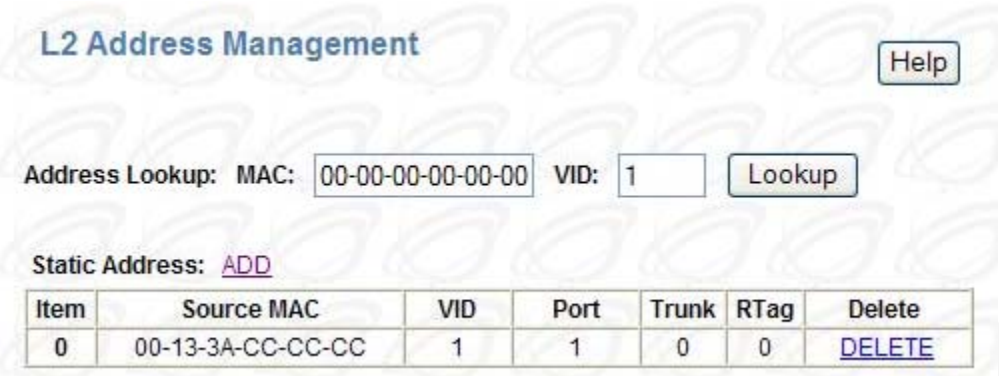


Figure 13: L2 Address Management

- **Add** inserts a new MAC address into the L2 address table.
- **Delete** removes the specified MAC address from the L2 address table.
- **Lookup** searches for the MAC address to determine whether it exists or not.

3.9.1 Add L2 Address

The configuration page assigns the information associated with the MAC address to the L2 address table.

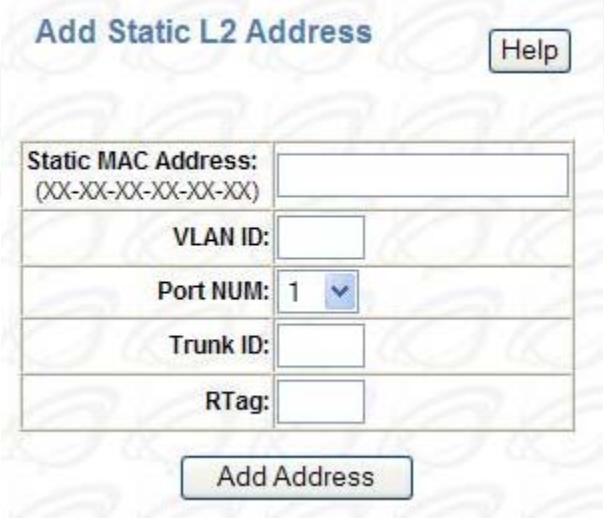


Figure 14: Add Static L2 Address

- **Static MAC Address** – Enter the Media Access Control (MAC) address.
- **VLAN ID** 802.1Q – Enter the VLAN ID.
- **Port NUM** – Select the port number.
- **Trunk ID** – If the address is in a trunk group, enter the trunk group ID of the MAC address.
- **RTag** specifies the packet distribution rule in this trunk if the MAC address is in a trunk group. RTag is used as the criterion to drive a trunk port index, which points to the egress port number in the trunk group. *SA* (Source Address), *DA* (Destination Address), or *SA*+*DA* fields can be used in the packets to decide the egress port in the trunk group.

3.9.2 Lookup L2 Address

Lookup Address Management searches for an existing L2 address.

3.10 Spanning Tree

The Rapid Spanning Tree Protocol (RSTP) provides rapid convergence of the spanning tree by assigning port roles and by determining active topology. The RSTP builds upon the IEEE 802.1D STP protocol to select the switch with the highest switch priority as the root switch. Reconfiguration of the spanning tree can occur in less than 1 second.

3.10.1 RSTP Switch Settings

The RSTP switch settings allow for the control of the RSTP parameters from the bridge point of view.

Figure 15: Rapid Spanning Tree

- **Designated Root Bridge** indicates the bridge identifier of the root of the spanning tree is determined by the RSTP protocol as executed by this node. The bridge identifier value is used as the root identifier parameter in all configuration bridge PCUs originated by this node.
- **Priority** indicates the priority of the root bridge.
- **Max Age** indicates the maximum age of the root bridge. This is the maximum age (measured in units of hundredths of a second) of spanning tree protocol information learned from the network on any port before it is discarded. This is the value that this bridge is currently using.
- **Hello Time** indicates the amount of hello time of the root bridge. Hello time is the amount of time (measured in units of hundredths of a second) between the transmission of configuration bridge PCUs by this node on any port when it is, or is trying to be, the root of the spanning tree.
- **Forward Delay** indicates the amount of forward delay of the root bridge. Forward delay is a time value, measured in units of hundredths of a second, which controls how fast a port changes its state. The value determines how long the port stays in each of the listening and learning states which precede the forward state. This value is also used to age all dynamic entries in the forwarding databases when a topology change has been detected and is underway.

3.10.2 RSTP Port Settings

RSTP port settings control and monitor port-based spanning tree status.

RSTP Port Settings Edit

Port	Name	Participate	Cost	Priority	Edge	P2P	Status	Role
1	AMC 1	☑ Yes	20000	128	Yes	Yes	Discarding	Disabled
2	AMC 2	☑ Yes	20000	128	Yes	Yes	Discarding	Disabled
3	AMC 3	☑ Yes	20000	128	Yes	Yes	Forwarding	Designated
4	AMC 4	☑ Yes	20000	128	Yes	Yes	Discarding	Disabled
5	AMC 5	☑ Yes	20000	128	Yes	Yes	Discarding	Disabled
6	AMC 6	☑ Yes	20000	128	Yes	Yes	Discarding	Disabled
7	AMC 7	☑ Yes	20000	128	Yes	Yes	Discarding	Disabled
8	AMC 8	☑ Yes	20000	128	Yes	Yes	Discarding	Disabled
9	AMC 9	☑ Yes	20000	128	Yes	Yes	Discarding	Disabled
10	AMC 10	☑ Yes	20000	128	Yes	Yes	Discarding	Disabled
11	AMC 11	☑ Yes	20000	128	Yes	Yes	Discarding	Disabled
12	AMC 12	☑ Yes	20000	128	Yes	Yes	Discarding	Disabled
13	MCH Management	☐ No	-	-	-	-	-	-
14	Front Panel	☑ Yes	200000	32	Yes	Yes	Forwarding	Designated
15	MCH Expansion	☑ Yes	20000	128	Yes	Yes	Discarding	Disabled
16	MCH Update	☑ Yes	20000	192	Yes	Yes	Discarding	Disabled

Apply Port Settings

Figure 16: RSTP Port Settings

- **Participate** specifies if the RSTP is enabled or not for the selected port.
- **Cost** displays the cost of this port. Cost is the contribution of this port to the path cost of paths toward the spanning tree root, which includes this port.
- **Priority** displays the priority of this port. This is the value of the priority field contained in the first octet of the port ID.
- **Edge** indicates if this port is the edge port. Once configured as an edge port, the port immediately transitions to the forwarding state.
- **P2P** indicates if this port is a point-to-point link. If a port is connected to another port through a point-to-point link and the local port becomes a designated port, it negotiates a rapid transition with the other port to ensure a loop-free topology.

- **Status** displays the RSTP port status. The following is the STP and RSTP spanning tree state mapping:

Spanning Tree Status	STP Port State	RSTP Port State
Enabled	Blocking	Discarding
Enabled	Listening	Discarding
Enabled	Learning	Learning
Enabled	Forwarding	Forwarding
Disabled	Disabled	Discarding

Table 2: RSTP and RSTP Spanning Tree State Mapping

- **Role** displays the role of this port. The RSTP provides rapid convergence of the spanning tree by assigning port roles and determining the active topology. The following describes the port roles:
    - *Root* port provides the best path (lowest cost) when the switch forwards packets to the root switch.
    - *Designated* port connects to the designated switch, which incurs the lowest path cost when forwarding packets from that LAN to the root switch.
    - *Alternate* port offers an alternate path (a path other than that provided by the current root port) toward the root switch.
    - *Backup* port acts as a backup for the path provided by a designated port toward the leaves of the spanning tree.
    - *Disabled* port has no role within the operation of the spanning tree.

3.11 802.1x

The IEEE 802.1X protocol is a standardized method for securing network access from the network devices. If a network user requires access to network server resources (file and print), then a login procedure must be successfully completed.

IEEE 802.1X operation denies unauthorized network access but does not withhold network traffic from authorized users.

3.11.1 Global RADUIS Setting

The RADIUS server is a Remote Authentication Dial-In User Service as defined in RFC2865. It is primarily used by ISPs that authenticate a username and password before authorizing the use of the network.

Figure 17: Global RADIUS Settings

- **Global RADIUS Setting** enables or disables global RADIUS operation.
- **RADIUS Server IP Address** specifies the IP address of the RADIUS server.
- **UDP Port Number** specifies User Datagram Protocol (UDP) port number of the EAPOL control frame; 1812 is the default UDP port number, but if the RADIUS server can recognize them, other numbers can be used.
- **Shared Secret** is a 16-character string used by the RADIUS server as a password to identify EAPOL control frames.

802.1X is a port-based authentication protocol. If a user port (supplicant) needs service from another port (authenticator), it must be verified and approved by the authenticator. The authenticator typically passes the Extensible Authentication Protocol (EAP) to an authentication server, which has all the security information. EAP is a high layer protocol used for authentication and it ensures mutual authentication between a wireless client and a server that resides at the network operations center. In order for layer 2 ports to participate in EAP protocol more efficiently, 802.1X creates another layer 2 protocol called EAPOL (EAP over LAN). With EAPOL, layer 2 can initiate or stop authentication functions. If a port needs service from another port, it needs to be authenticated by that port. EAPOL is the protocol used for this authentication process.

Extensible Authentication Protocol over LAN (EAPOL) is the key protocol in 802.1X as it provides effective authentication regardless of whether 802.11 WEP keys or any encryption are implemented. If configured to implement dynamic key exchange, the 802.1X authentication server can return session keys to the access point along with the accept message. The access point uses the session keys to build, sign, and encrypt the EAP key message that is sent to the client immediately after sending the success

message. The client can use the contents of the key message to define applicable encryption keys.

3.11.2 Port Authentication Setting

The Port Authentication function establishes security between ports. It also displays the result when a port is enabled for authentication.

Port	Name	Set Status	Show Client MAC	Authorization
1	AMC 1	☐ Disabled		N/A
2	AMC 2	☐ Disabled		N/A
3	AMC 3	☐ Disabled		N/A
4	AMC 4	☐ Disabled		N/A
5	AMC 5	☐ Disabled		N/A
6	AMC 6	☐ Disabled		N/A
7	AMC 7	☐ Disabled		N/A
8	AMC 8	☐ Disabled		N/A
9	AMC 9	☐ Disabled		N/A
10	AMC 10	☐ Disabled		N/A
11	AMC 11	☐ Disabled		N/A
12	AMC 12	☐ Disabled		N/A
13	MCH Management	☐ Disabled		N/A
14	Front Panel	☐ Disabled		N/A
15	MCH Expansion	☐ Disabled		N/A
16	MCH Update	☐ Disabled		N/A

Apply Port Settings

Figure 18: Port Authentication Setting

- **Set Status** enables or disables port authentication. Enable port authentication means these ports should be authorized by a RADIUS server to forward traffic. No unauthorized traffic is forwarded. No authentication process is required for those ports in disabled status; traffic can be forwarded normally.
- **Show Client MAC** displays the last client in the MAC address that sent out the EAPOL control from of the port.
- **Authentication** displays the authentication status of an enabled port.
    - *Yes* indicates the authentication has passed; the traffic is allowed to be forwarded.
    - *No* indicates the authentication has failed; the traffic is not allowed to be forwarded.
    - *In Progress* indicates that the authentication is still in progress. Traffic is not forwarded before authentication is verified.
    - *N/A* is defined as no authentication required.

3.12 IGMP Snooping

IGMP is a standard defined in RFC1112 for IGMPv1 and in RFC2236 for IGMPv2. IGMP specifies how a host can register a router in order to receive specific multicast traffic. Configure the switch to use IGMP snooping in subnets that receive IGMP queries from either IGMP or the IGMP snooping querier. IGMP snooping constrains multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward multicast traffic only to those ports that want to receive it.

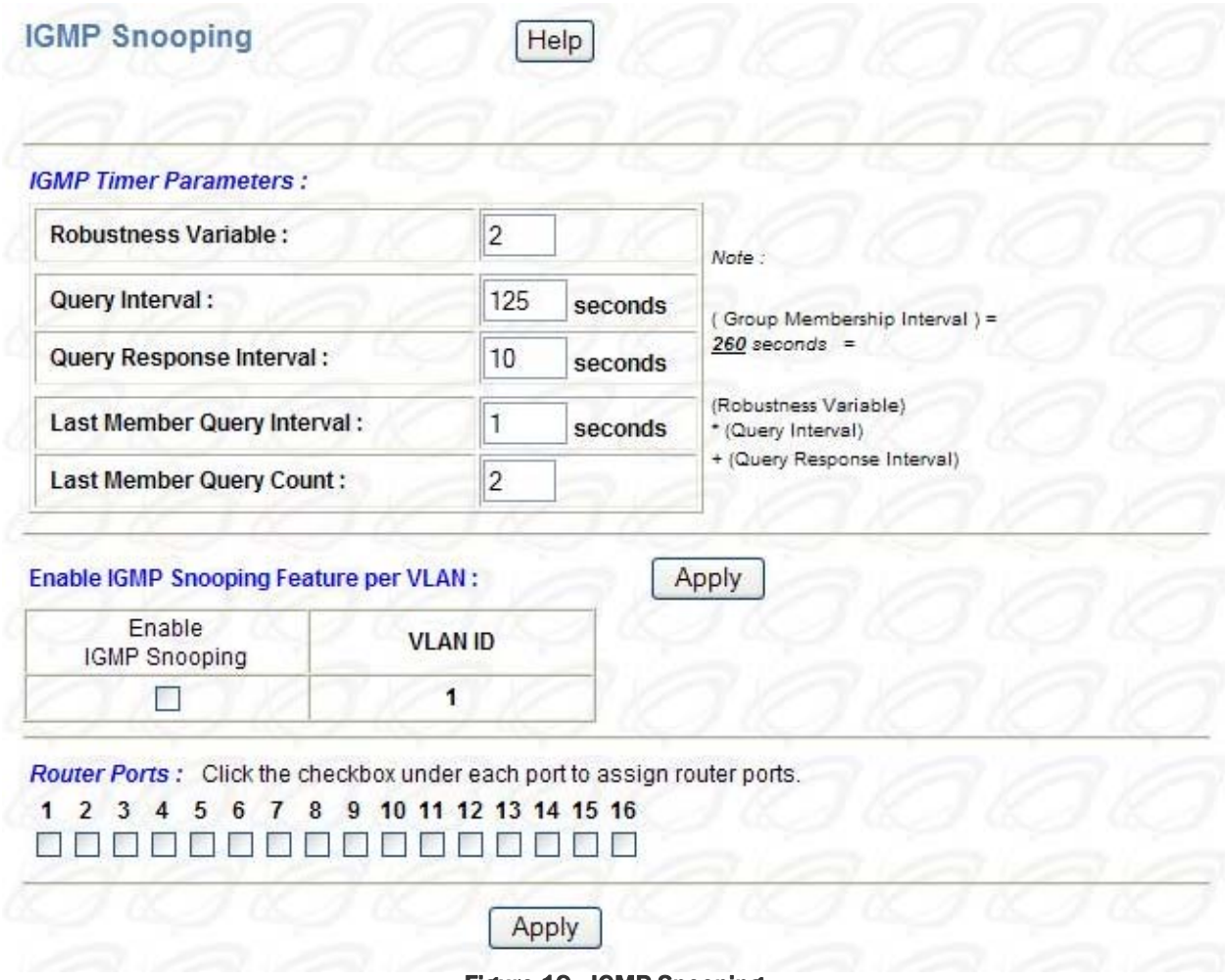


Figure 19: IGMP Snooping

- **Enable IGMP Snooping** enables or disables the IGMP snooping feature.
- **Robustness Variable** allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the robustness variable may be increased. IGMP is robust to (Robustness Variable – 1) packet losses. The robustness variable must not be 0, and should not be 1. The default value is 2.
- **Query Interval** is the interval between general queries sent by the querier. The default interval is 125 seconds. By varying the Query Interval, an administrator may

fine tune the number of IGMP messages on the subnet; larger values cause IGMP queries to be sent less often.

- **Query Response Interval** is the maximum response time inserted into the periodic general queries. The default value is 100 (10 seconds). By varying the query response interval, an administrator can fine tune the level of the burst of IGMP messages on the subnet; larger values create less of a traffic burst, as host responses are spread out over a larger interval. The number of seconds represented by the query response interval must be less than the query interval.
- **Last Member Query Interval** is the maximum response time inserted into group-specific queries sent in response to Leave Group messages, and is also the amount of time between group-specified query messages. The default value is 10 (1 second). This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group.
- **Last Member Query Count** is the number of group-specific queries sent before the router assumes there are no local members. Default: the Robustness Variable.
- **Enable IGMP Snooping Feature per VLAN** enable or disable the IGMP snooping feature for a specific VLAN. All VLAN IDs created are listed here. This feature is disabled by default for a newly created and default VLAN IDs.
- **Router Ports** specifies the ports to which IGMP routers are connected.

3.13 Auto DoS

Denial-of-service (DoS) attack prevention is a method of preventing an attack on a computer system or network that causes a loss of service to users. Typically, a DoS attack causes the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim's system.

3.13.1 Global Auto DoS Attack Prevention

Figure 20: Global Auto DoS

The following attack packets can be prevented:

- **Land Attack** – Packets with the source IP equals the destination IP.
- **Blat Attack** – Packets with the source port equals the destination port.
- **NULL scan** – TCP sequence number is zero and all control bits are zeros.
- **SYN with sport < 1024** – SYN packets with a source port less than 1024.
- **Xmascan** – Sequence number is zero and the FIN, URG and PSH bits are set.
- **SYNFIN** – SYN and FIN bits that are set in the packets.
- **Ping of Death Attacks** – Using packets larger than 64K bytes through fragments and target the vulnerable systems.
- Click **Advanced** to set additional per-port DoS attack prevention.

3.13.2 Per-Port DoS Attack Prevention

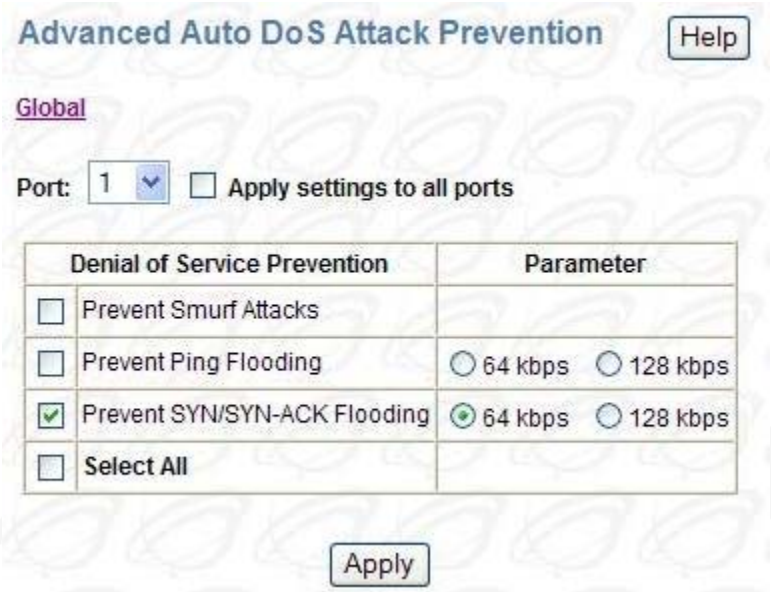


Figure 21: Per-Port Auto DoS

- **Smurf Attack** – Ping packets attacks that can cause network congestion or outages.
- **Ping Flooding** – Flooding of ICMP packets.
- **SYN/SYN-ACK** – Flooding of SYN or SYN-ACK packets.
- **Limit** – Limit the rate for Ping Flooding and SYN/SYN-ACK.

3.14 Auto VoIP

Voice over Internet Protocol (VoIP) allows telephone calls to be made using a computer network over a data network like the Internet. With the increased prominence of delay-sensitive applications (voice, video, and other multimedia applications) deployed in networks today, proper QoS configuration ensures high-quality application performance. The Auto VoIP feature is intended to provide an easy classification mechanism for voice packets so that they can be prioritized above data packets in order to provide better QoS.

The Auto VoIP module explicitly matches VoIP streams in Ethernet switches and provides them with a better class of service than ordinary traffic. The Auto VoIP module provides the capability to assign the highest priority for the following VoIP packets:

- *SIP* – Session Initiation Protocol
- *MGCP* – Media Gateway Control Protocol
- *SCCP* – Skinny Call Control Protocol

Figure 22: Auto VoIP

- **Profiles** indicates the current profile to control; Disable does not select any profile.
- **Guaranteed bandwidth** indicates the guaranteed minimum bandwidth for traffic of the selected profile.

3.15 Logging

Event logs are used to record various system events. By properly configuring the logging system, users can control the type of log messages that can be recorded. To configure the level of logs to be recorded, select the appropriate levels (Error/Warning/Info/Debug) for each logging target then press the **Apply** button.

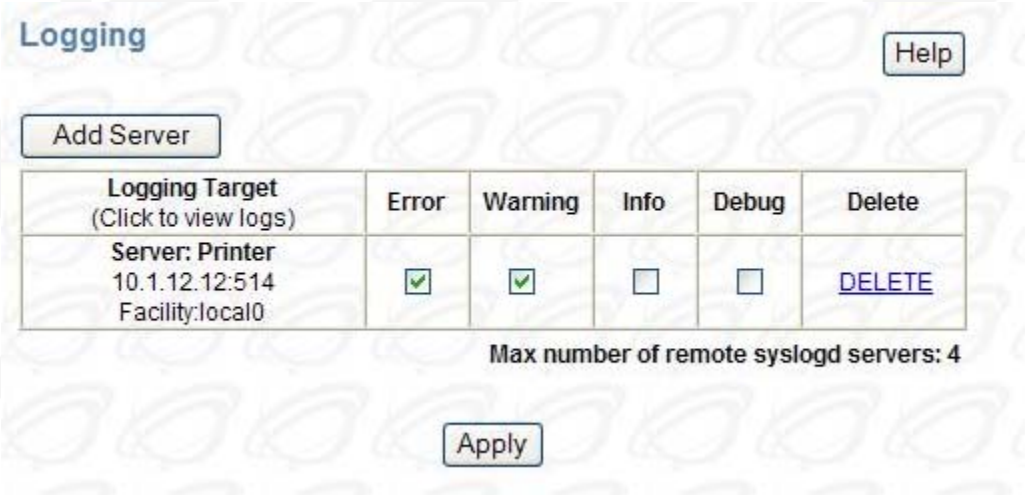


Figure 23: Logging

For a remote syslogd-based server, users can click the **Add Server** button to supply the new server information.

Figure 24: Add Logging Server

- **Name** specifies a short name or description for identifying this server.
- **IP Address** specifies the IP address of the server (in dotted decimal notation).
- **Port** specifies the UDP port of the server (normally 514 for syslogd).
- **Facility** specifies the facility value to be used when logs are recorded in the remote server. See RFC3164 for reference.

Index