DG-IES-EN2503M
Managed Media Converter
Web Operation Manual

Contents

1 Production introduction

1.1 Overview

DG-IES-EN2503M managed Media Converter can provide 2*GE ports, 1*GFX ports, GE ports support 100/1000M-TX ports with AUTO-negotiation, GFX support 1000Base-X, and fixed with SFP ports. Stable system make sure the Network more safety and reliable.

Firmware feature

- Network management: Web, Telnet, Console
- Switch attribute: VLAN, Qos
- Redundancy protocol: ERPS, MSTP/RSTP/STP, Ring
- Multicast: IGMP Snooping,static multicast, MLD Snooping
- Network security: ACL
- Network surveillance: SNMP v1/v2/v3,RMON
- Bandwidth management: link aggregation, port speed limit
- Diagnosis: mirroring, LLDP

Technical Standard

- IEEE 802.3 10Base-T 10Mbit/s Ethernet
- IEEE 802.3u 100Base-TX, 100Base-FX, Fast Ethernet
- IEEE 802.3ab 1000Base-T Gbit/s Ethernet over twisted pair
- IEEE 802.3z 1000Base-X Gbit/s Ethernet over Fiber-Optic
- IEEE 802.1d STP (Spanning Tree Protocol)
- IEEE 802.1w RSTP (Rapid Spanning Tree Protocol)
- IEEE 802.1s MSTP (Multiple Spanning Tree Protocol)
- ITU-T G.8032 / Y.1344ERPS (Ethernet Ring Protection Switching)
- IEEE 802.1Q Virtual LANs (VLAN)
- IEEE 802.1X Port based and MAC based Network Access Control, Authentication
- IEEE 802.3ad Link aggregation for parallel links with LACP(Link Aggregation Control Protocol)
- IEEE 802.3x Flow control for Full Duplex
- IEEE 802.1ad Stacked VLANs, Q-in-Q
- IEEE 802.1p LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization
- IEEE 802.1ab Link Layer Discovery Protocol (LLDP)

- IEEE 802.3az EEE (Energy Efficient Ethernet)

2 DG-IES-EN2503M managed Media Converter access

1) Web
2) Console port
3) Telnet

If equipment IP address is unknown, you can connect Console to PC to get it, the default IP is 192.168.0.2.

2.1 Web access

Enter the IP address in the browser's address bar, the login screen is displayed, then enter the user name "admin" and default password is 123. as shown in figure 2-1 below:

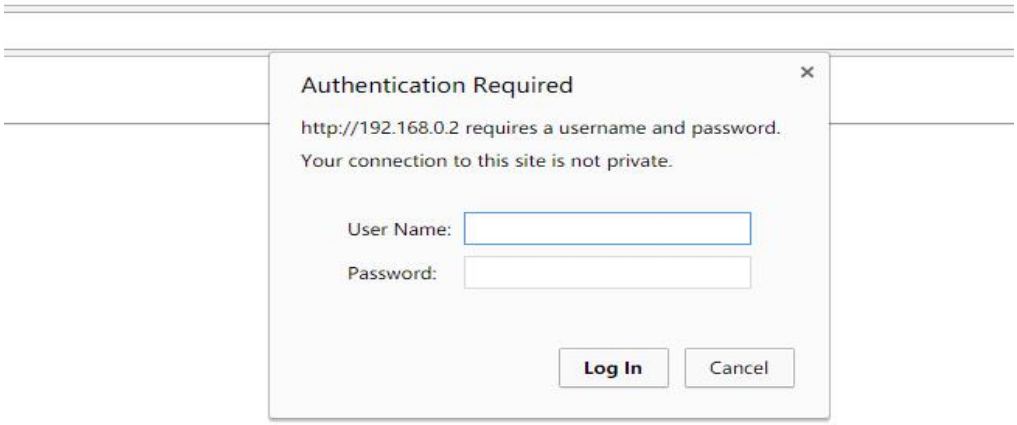

Figure 2-1 login interface

When you logged in to web interface, as shown in figure 2-2, it's navigation menu on the left and detailed interface on the right.

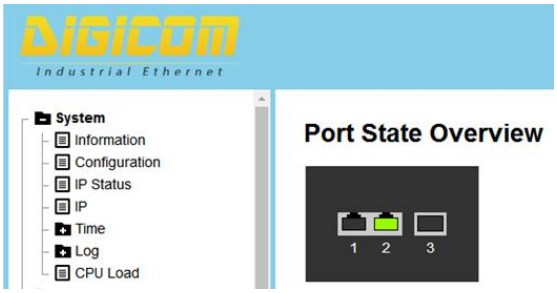

Figure 2-2 Web interface

2.2 Console port access

User can use hyper terminal of Windows or other softwares that support serial connection such as xshell to access media converter via Console port. The following example shows how to use hyper terminal to access the switch via Console port:

(1) Connect the PC serial port to switch Console port via DB9 cable we offered.

(2) Run the hyper terminal from Windows,click Start→All programmes→ Accessories→ Communications→Hyper terminal

(3) Create a new connection “switch”, as shown in figure 2-3:

Figure 2-3 new connection

(4) choose COM1 as shown in figure 2-4.

Notes: please check device manager to confirm the corresponding COM port.

Figure 2-4 COM port selection

(5) COM1 setting as shown in figure2-5, Bit/s(baud rate: 115200; Data bits: 8; Parity: None; Stop bits: 1; Flow control: None

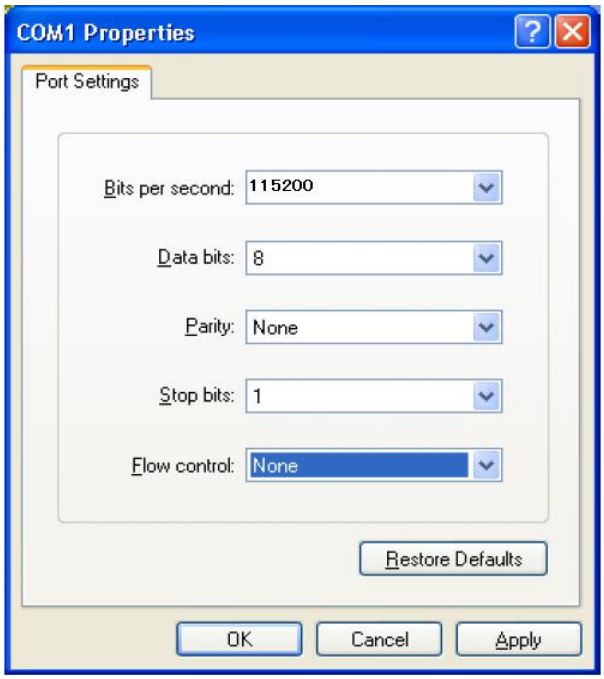

Figure 2-6 Serial port setting

(6) Click “OK” to enter into CLI, the default user name of serial management is “admin”,the default password is “123”. as shown in figure2-6.

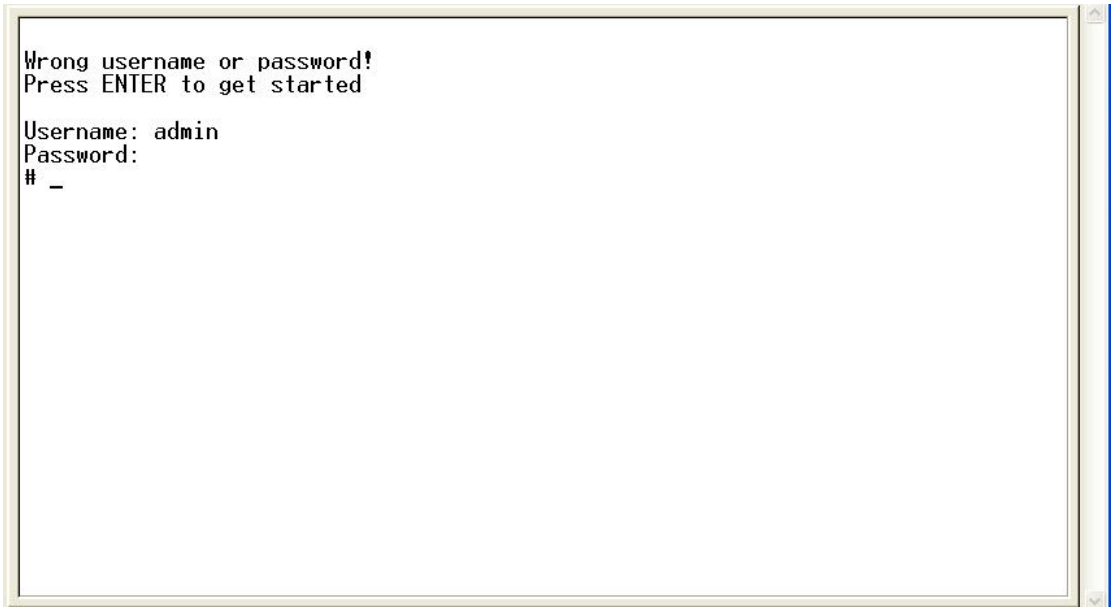

Figure 2-6 CLI

2.3 Telnet access

PC and switch IP address shall be in the same network when accessing the Telnet. Type “telnet IP address” in the run dialogue as shown in figure 2-7.

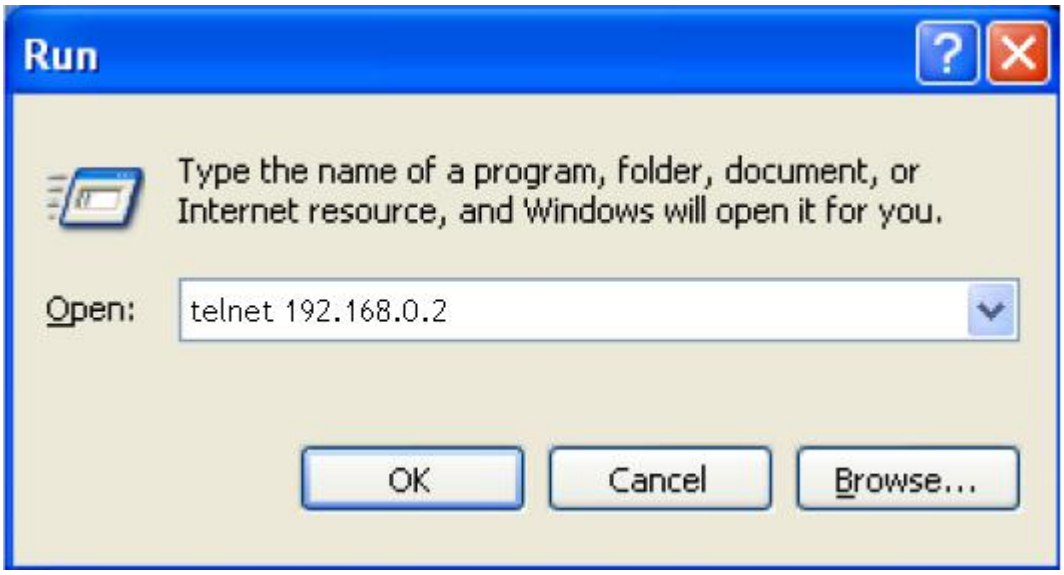

Figure 2-7 Telnet access

Type user name “admin” and password is “123” in Telnet interface and press <Enter> to log in Telnet CLI as shown in figure 2-8.

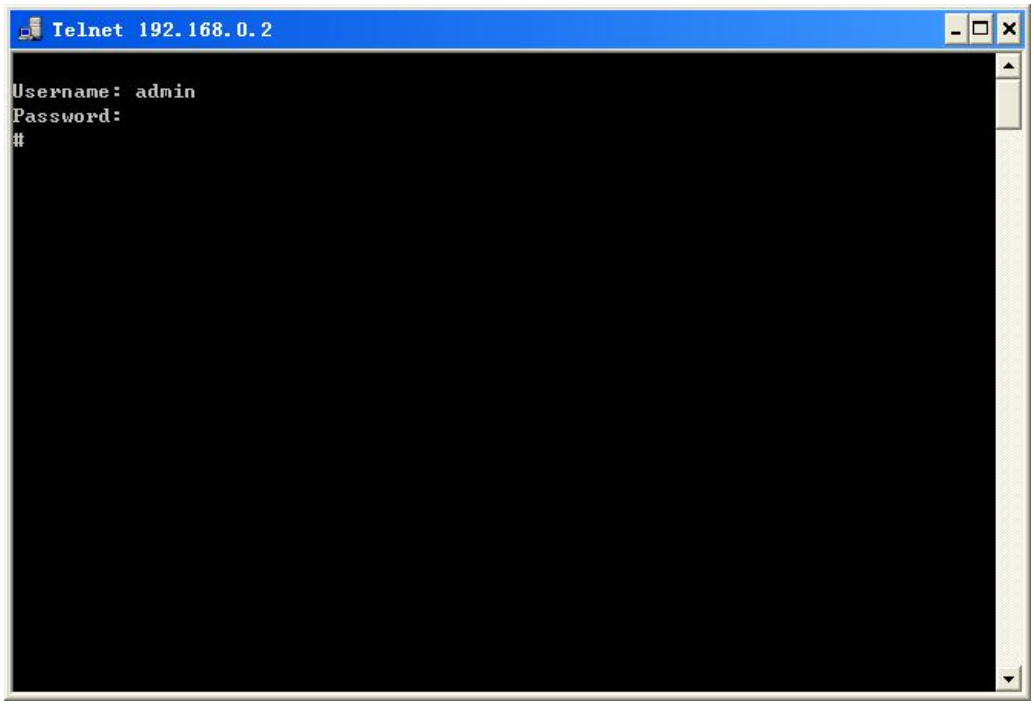

Figure 2-8 Telnet CLI

3 Equipment management

3.1 Basic information

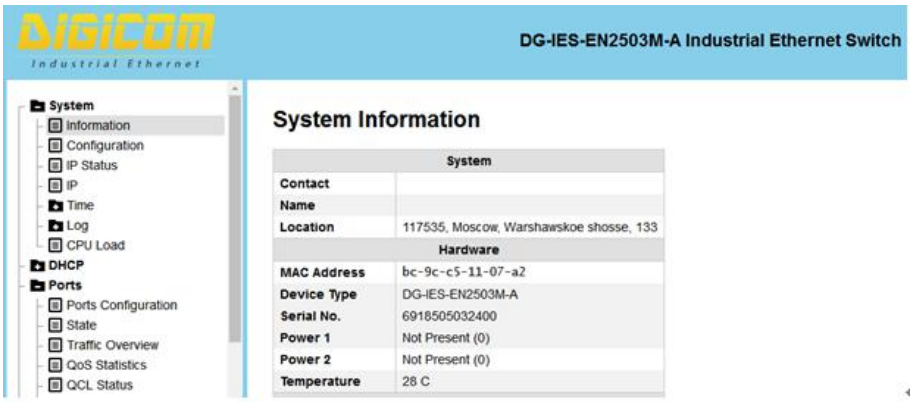

Figure 3-1 basic information

System Contact

The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

System Name

The allowed string length is 0 to 255.

System Location

The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

3.2 IP address change

Management IP address can be changed as shown in figure 3-2.

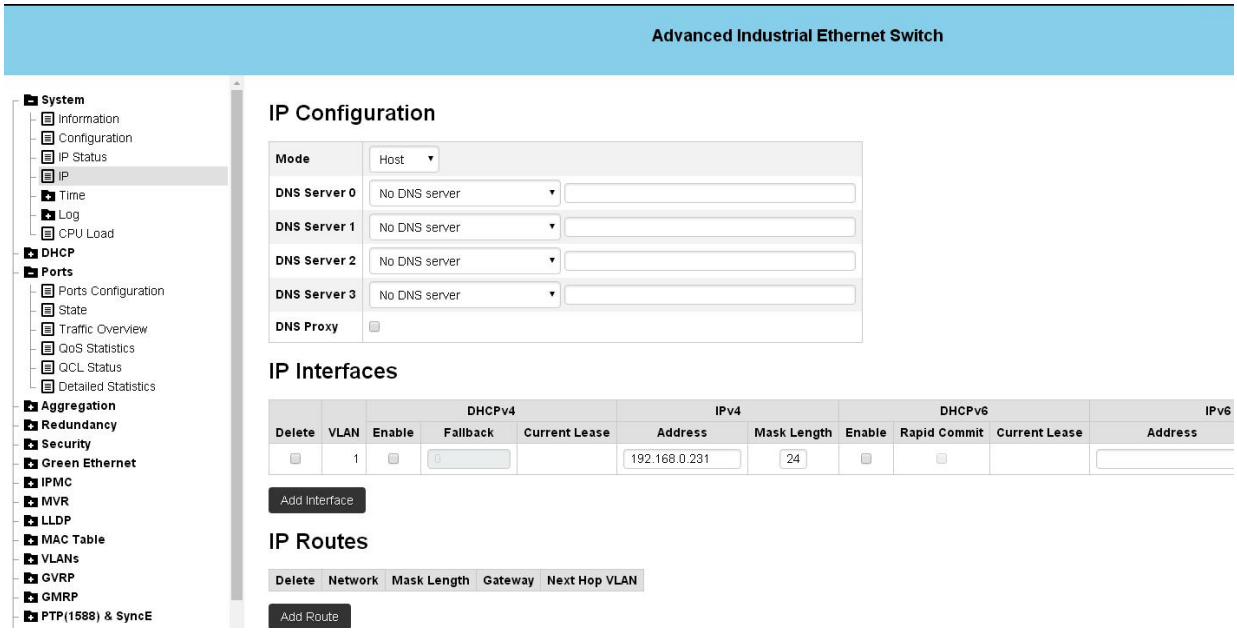

Figure 3-2 IP address change

3.3 Firmware update

Software upgrades, as shown below. Click “Browse” to locate the firmware in the format '.dat'.

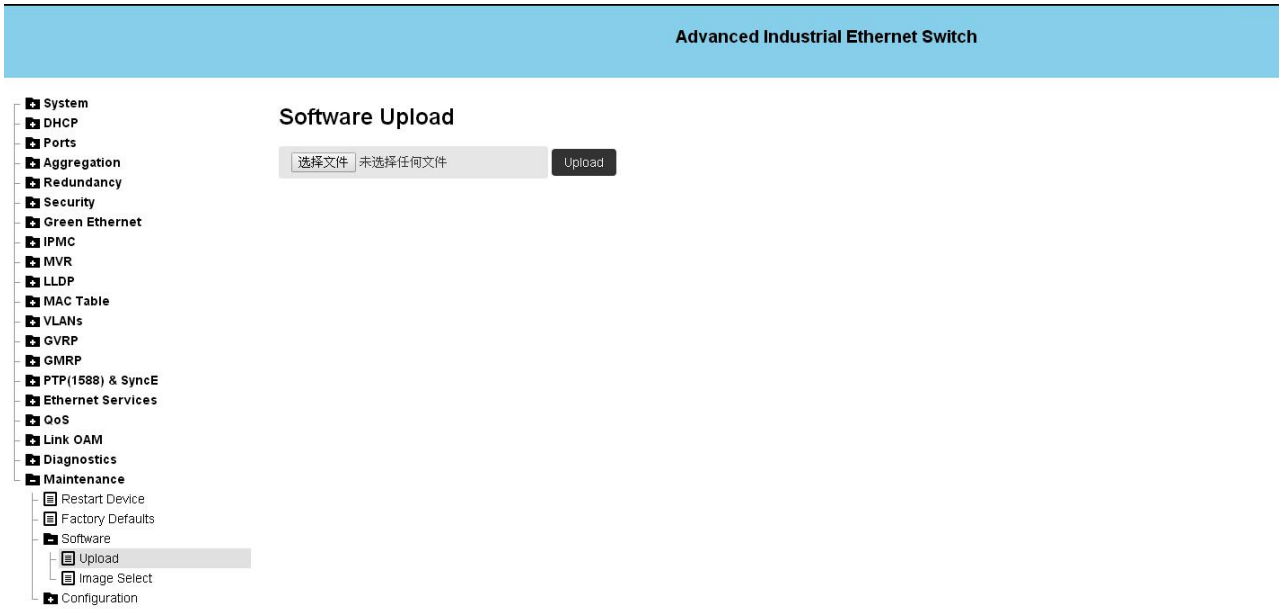

Figure 3-3 Software update

Browse and select the software that needs to be updated, click Upload, as shown in Figure 3-4.

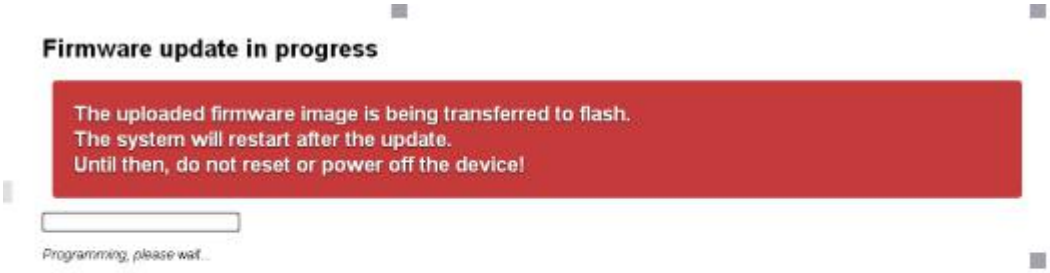

Figure 3-4 Firmware update in progress

4 Ports Configuration

This page can be configured with speed, flow control, maximum frame size, etc., as shown in Figure 4-1

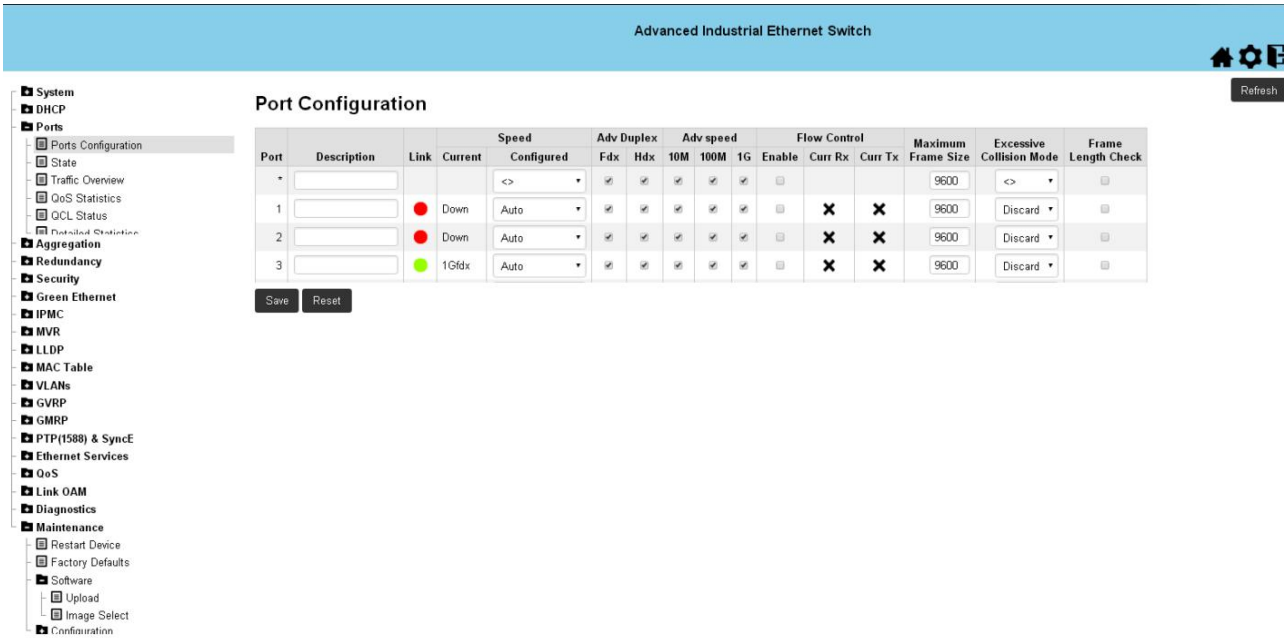

Figure 4-1 Mode configuration

When you have any doubt, you can click the button like  at the top right of the web to get the help. shown in figure 4-2.

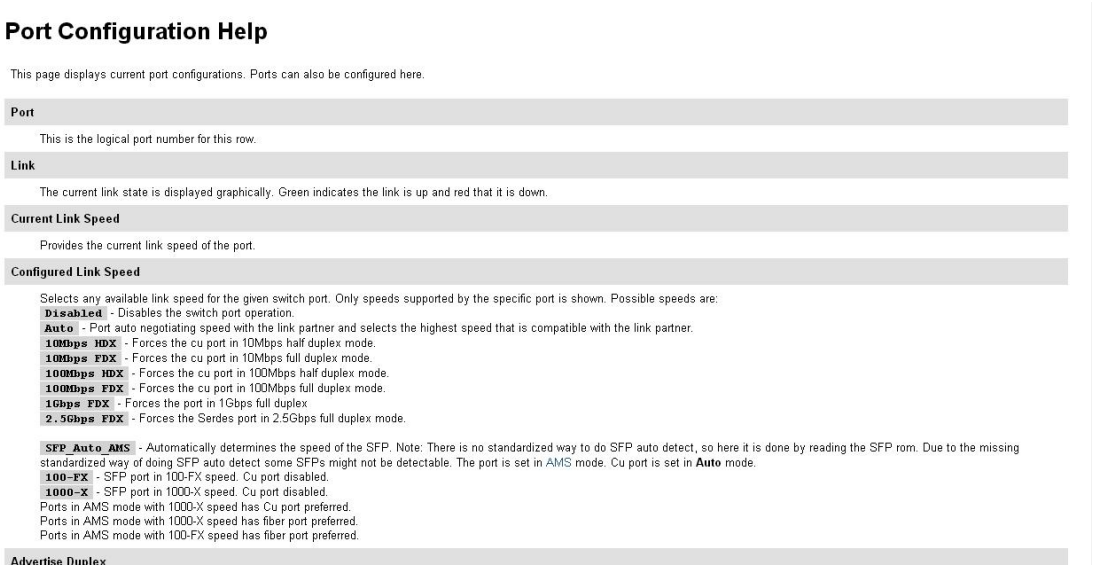

Figure 4-2 Help

5 VLAN

5.1 Global VLAN Configuration

Add VLAN 2,3

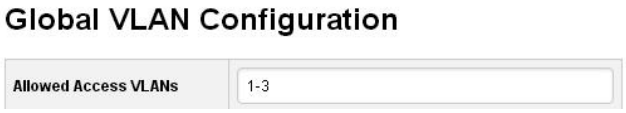

Figure 5-1 add VLAN

Delete VLAN2

Figure 5-2 delete VLAN

Show Existing VLAN

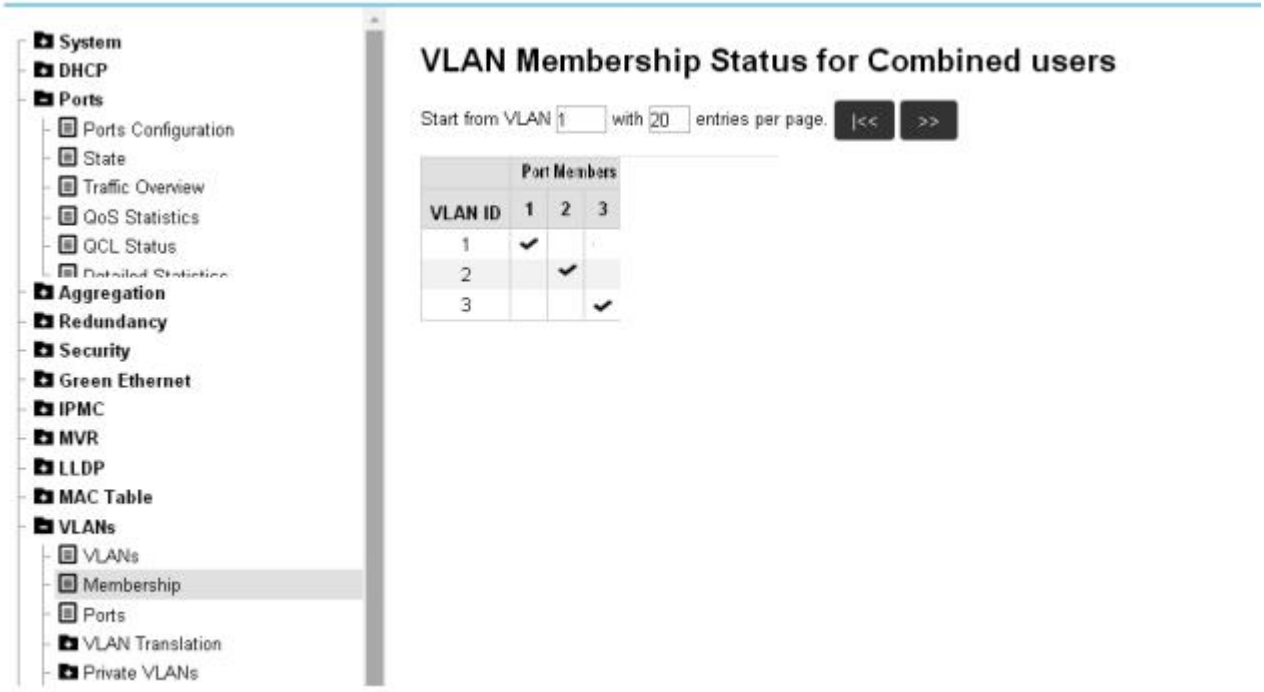

Figure 5-3 show existing VLAN

5.2 Port VLAN Configuration

The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below.

Access:

- Access ports can belong to only one VLAN
- Accept unlabeled frames and C-tagged frames,
- Discard frames that do not belong to the VLAN,
- At the exit, all frames are transmitted without tags.

Trunk:

Trunk ports can belong to multiple VLANs at the same time. Usually used to connect to other switches. The Trunk port has the following features:

By default, the trunk port belongs to all VLANs. You can configure the trunk port.

By default, the packets coming from the trunk port carry the tag (except that the VLAN of the packet is equal to the default PVID).

Hybrid:

Hybrid ports A hybrid port can allow multiple VLANs to pass through, receive and send packets of multiple VLANs. It can be used to connect between switches and to connect to a user's computer.

5.2.1 Allowed VLANs

Ports in Trunk and Hybrid modes can control which VLANs are allowed to become members. The access port can only be a member of a VLAN, that is, an access VLAN.

5.2.2 Quick configuration example

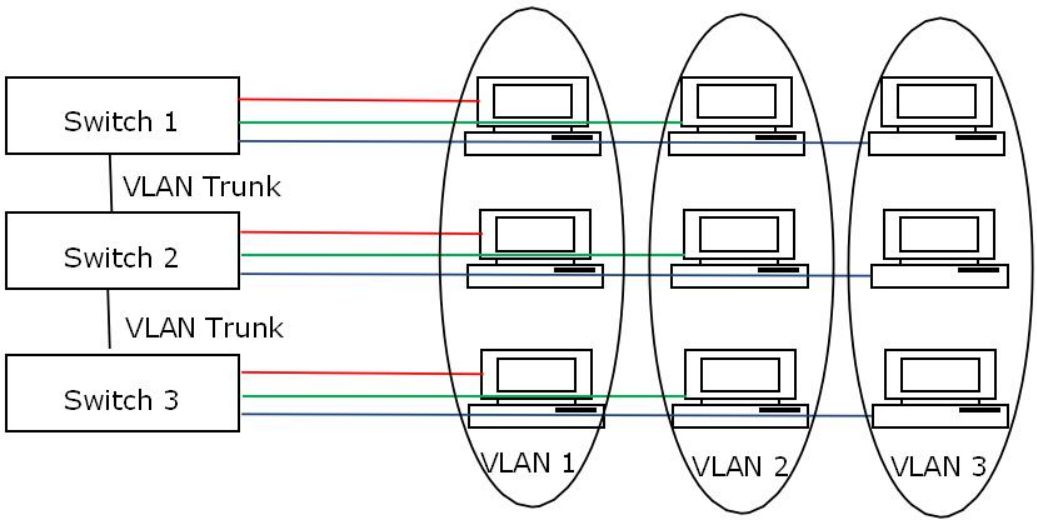

Figure 5-4 Quick configuration example

Global VLAN Configuration

Allowed Access VLANs	1-3
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs
*	<>	1	<>	☑	<>	<>	1
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1
2	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3
3	Access	3	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3

Figure 5-5 Port VLAN configuration

6 QoS configutation

6.1 QOS Implementation

6.1.1 QOS Classification

In frame basic and advanced hierarchies, there are two methods for classifying into QoS classes and for re-marking priority information.

Basic QOS Classification

Basic QoS classification based on PCP, DEI, SCP:

- QoS classification of PCP and DEI based on tagged frames. Each port from PCP and DEI to QoS level mapping can be modified.
- QoS classification based on DSCP values.
- DSCP conversion
- DSCP mark based on QOS level.
- QOS class configuration for unlabeled and non-IP packets.

Advanced QOS Classification

Advanced QoS grading using QCL to provide flexible rating:

- High-level protocol fields for rule matching.
- Operations include mapping to QOS classes and converting PCP, DEI and DSCP values

6.1.2 Policers

The governor limits the bandwidth of the receive frame beyond the configurable rate. The governor can be configured at the queue level or at the port level.

6.1.3 Scheduling algorithm

There may be two types of scheduling on a port-level switch.

Strict priority

All queues follow strict priority

DWRR

Scheduled based on the weights configured for each queue. Queues 6 and 7 always use strict priorities for

scheduling. DWRR can be done on a queue of 0 to 5.

6.2 QOS Classification

6.2.1 Basic QOS Classification

Port Classification

Ports can assign QOS levels (CoS), PCP, DPL, and DEI to ingress packets.

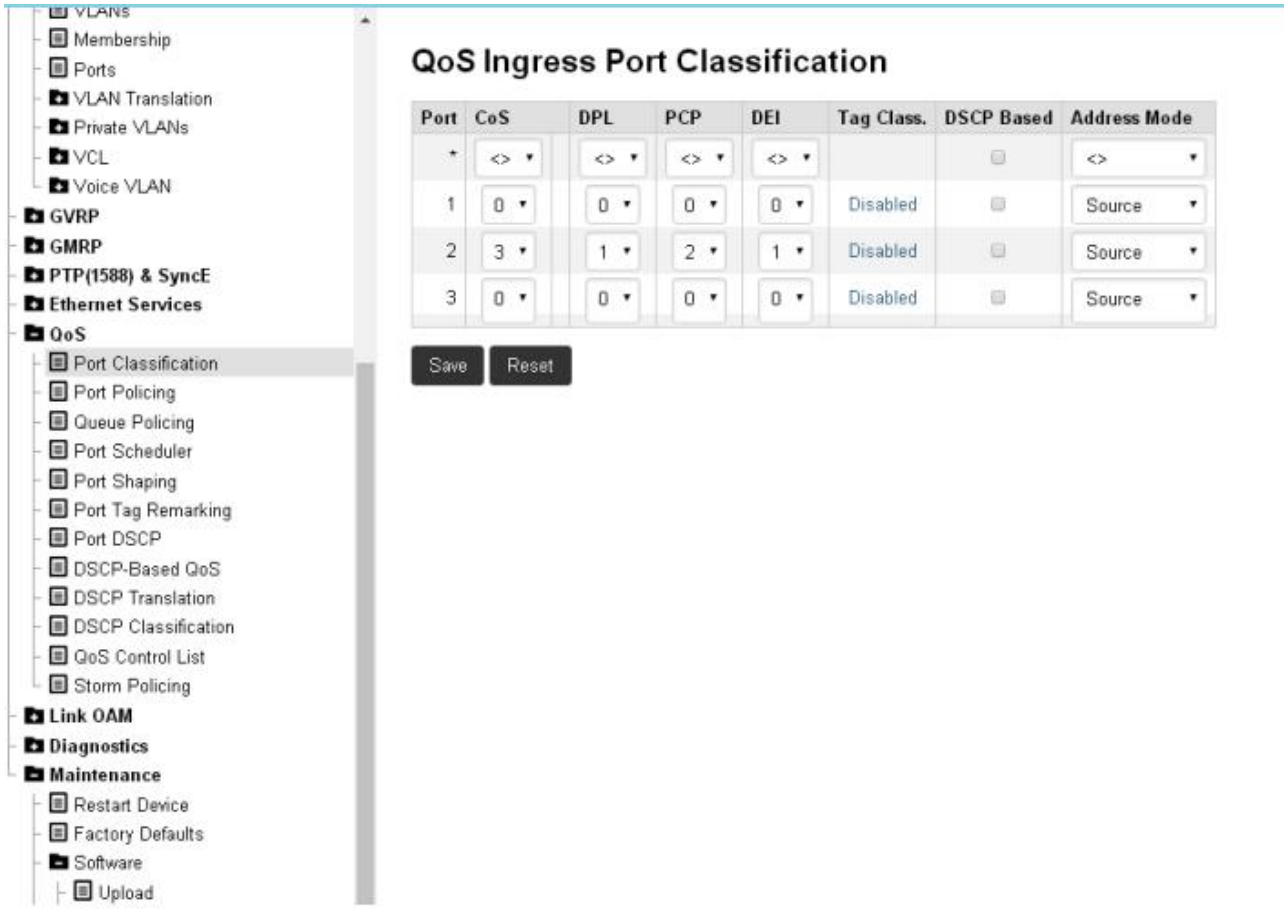

Figure 6-1 Port Classification

6.2.2 Port tag reset

There are three ways to tag tag in outgoing direction:

1. **Classifed**: The PCP and DEI values of the packets in the Egress direction can be updated by the corresponding value in the Ingress direction.

2. **Default**: PCP and DEI values of Egress packets can use the default values defined by the port.

3. **Mapped**: PCP and DEI values of Egress packets are updated according to the mapping of tags.

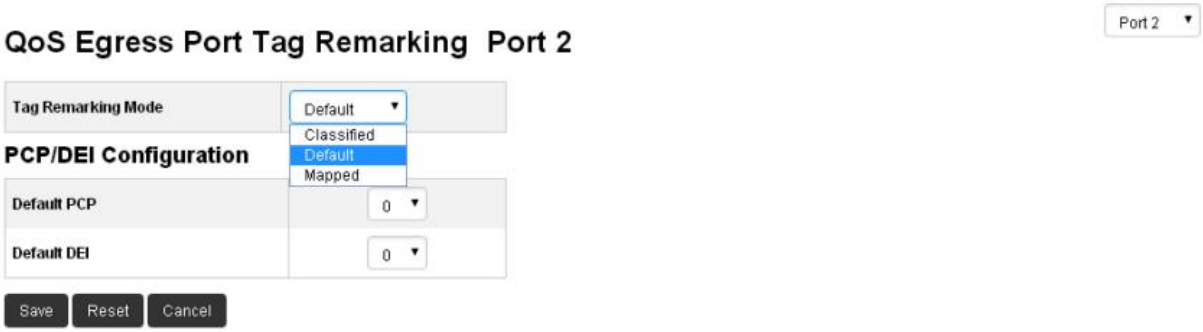

Figure 6-2 QoS Ingress Port tag

Mapping QoS Class 2 and DPL 0 to PCP 3 and DEI 0, mapping Qos Level 3 and DPL 1 to PCP 4 and DEI 1. As shown figure 6-3.

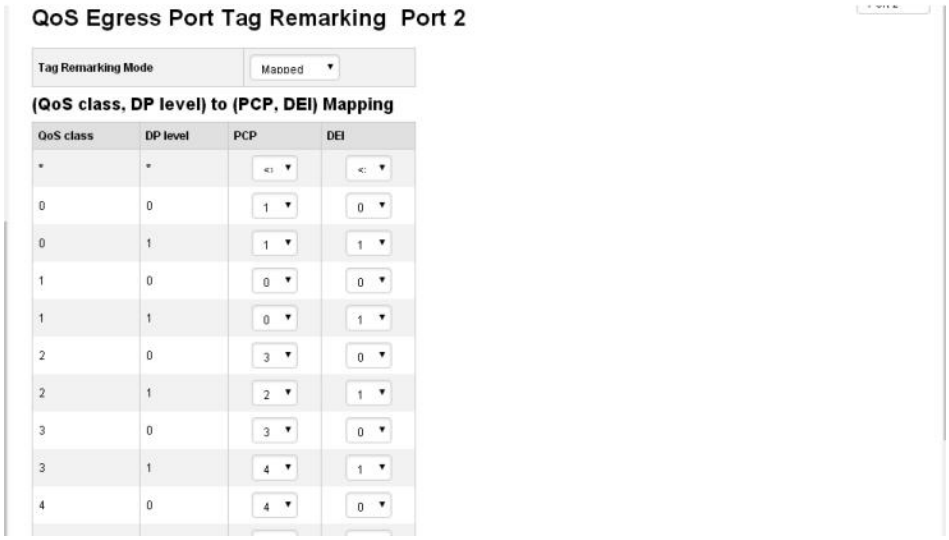

Figure 6-3 QoS Egress port tag

6.2.3 DSCP Configuration

DSCP Configuration per port is present both on ingress and egress.

Port 2 is based on DSCP-based QoS classification in the Ingress direction, as shown in Figure 6-4.

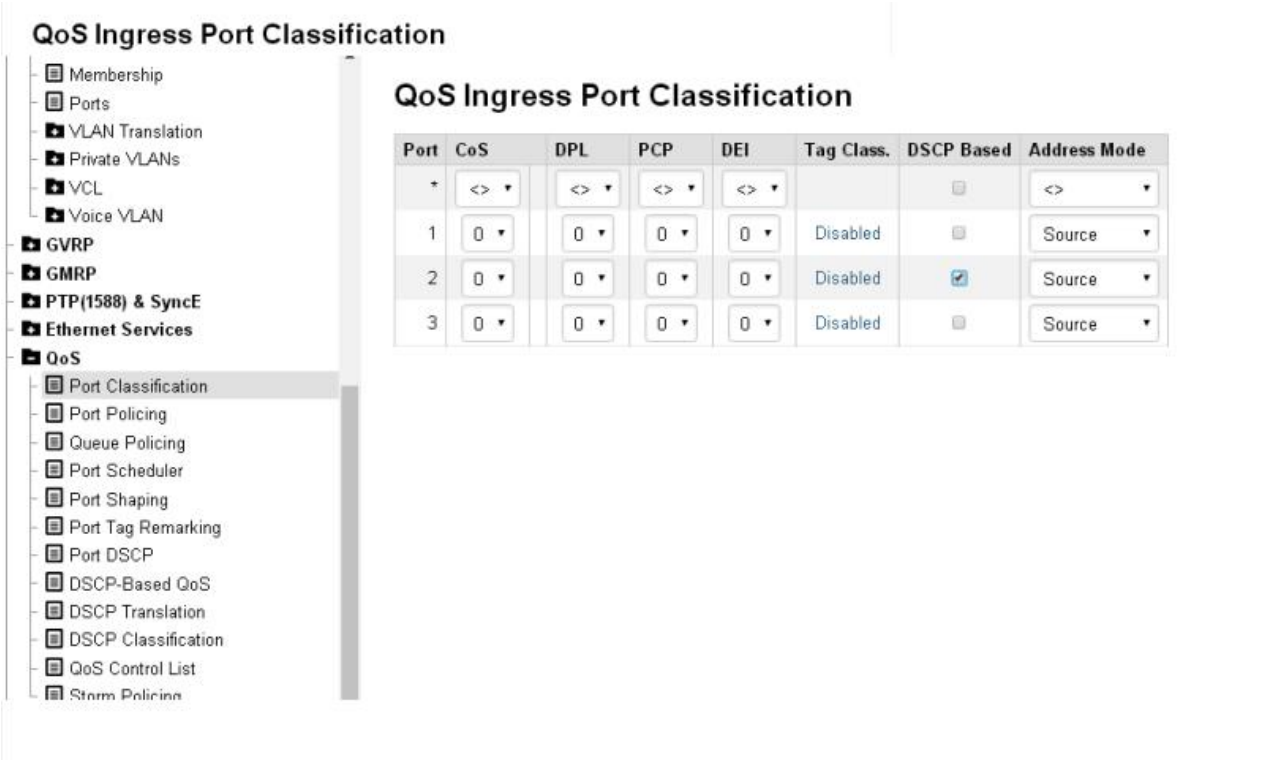

Figure 6-4 QoS ingress port classification

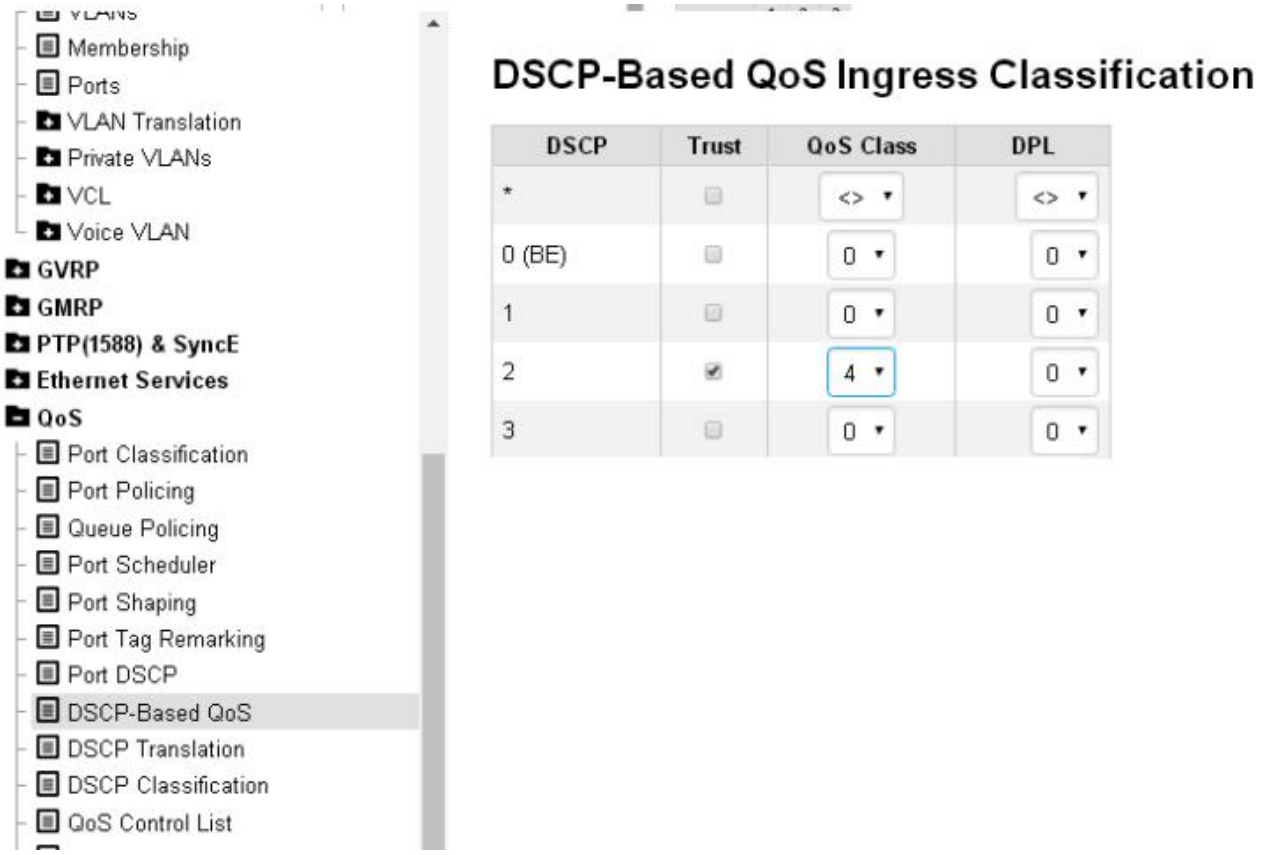

Figure 6-5 DSCP-Based QoS Ingress Classification

Translate DSCP at ingress of port 2 and rewrite enabled on port 3, as shown in Figure 6-6.

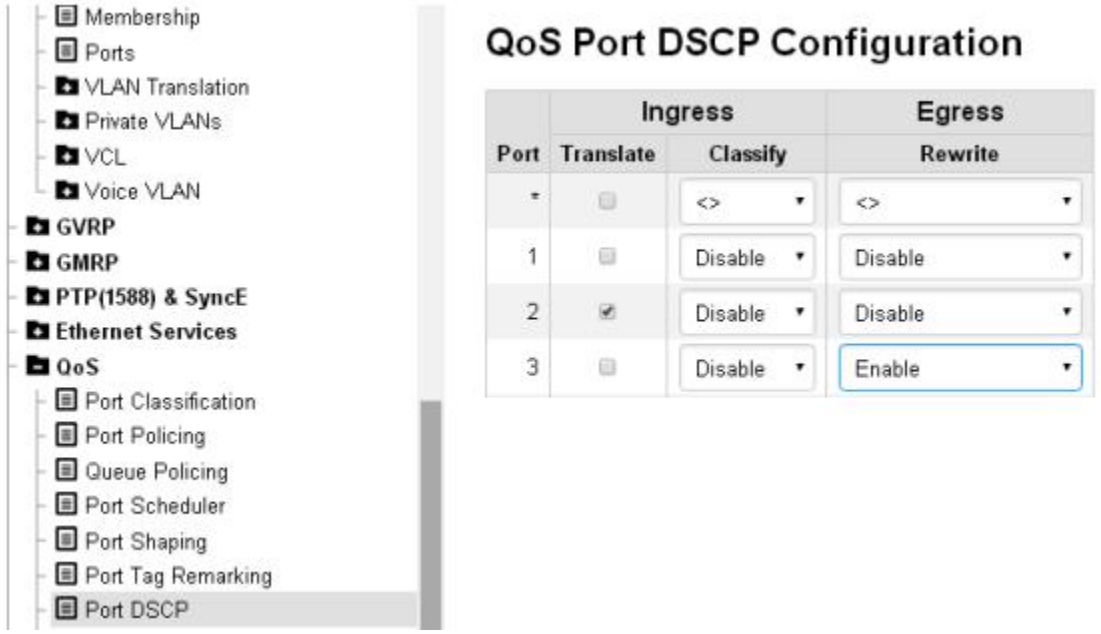

Figure 6-6 QoS port DSCP configuration

Set DSCP=0 at ingress of port 2 and rewrite enabled on port 3.

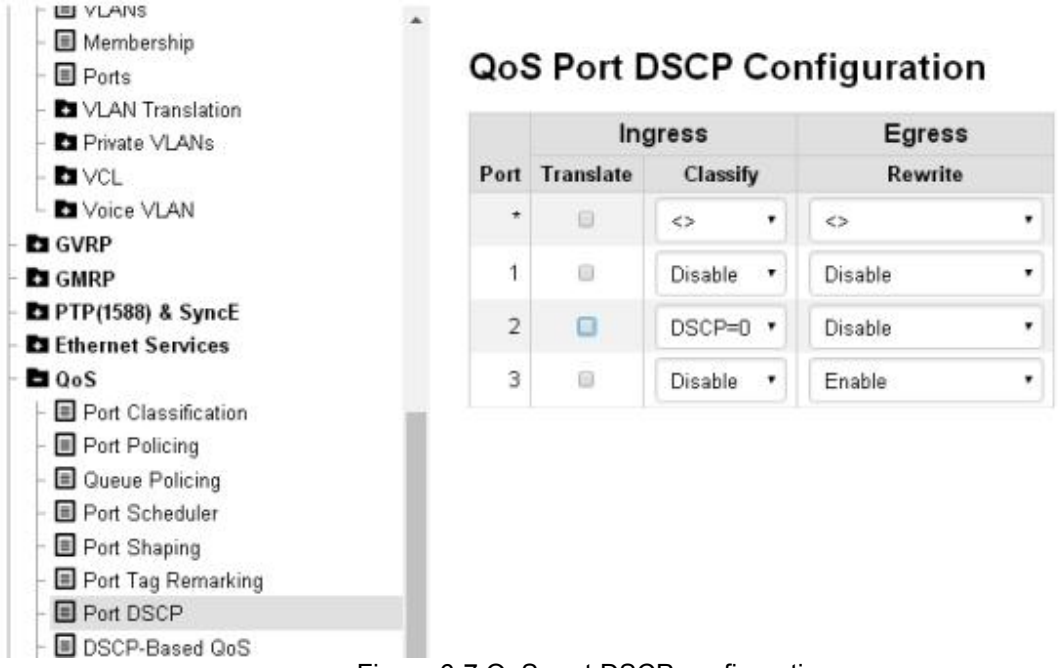

Figure 6-7 QoS port DSCP configuration

6.3 Advanced QOS Classification

6.3.1 QCLs

Advanced QOS classification can be done by checking the packets, and mapping them to PCP/DEI, QOS class, and DSCP values.

Match specific source MACs on port 2 and map these to QoS class 5, as shown in Figure 6-8.

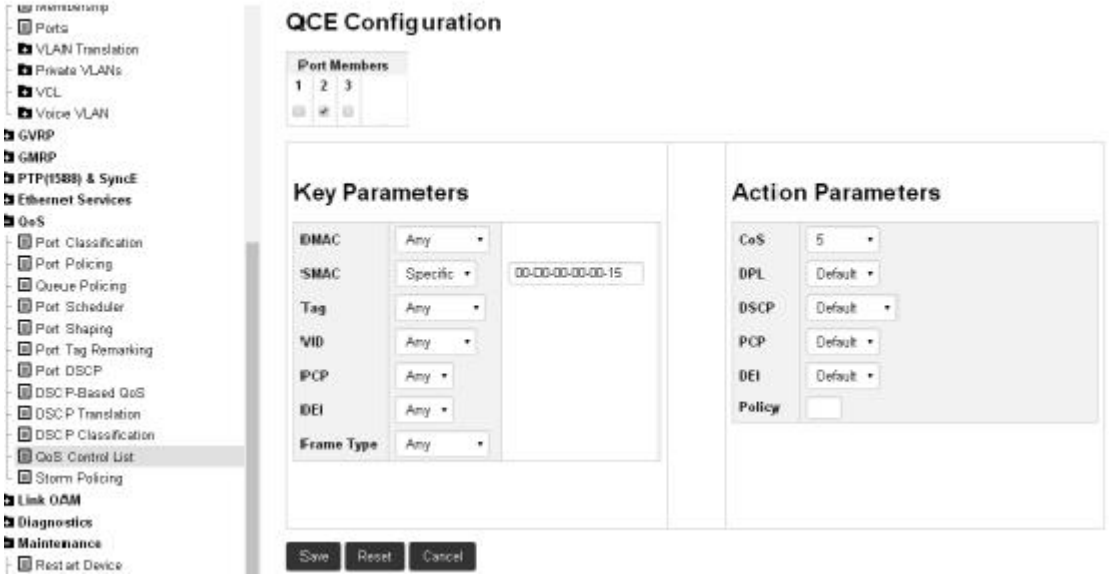

Figure 6-8 QCE configuration

6.3.2 Policers

6.3.2.1 Port Policers

Enable the policy at the port level on a specific port

Enable the policy on port 2 and set the rate to 2000Kbps, as shown in Figure 6-9.

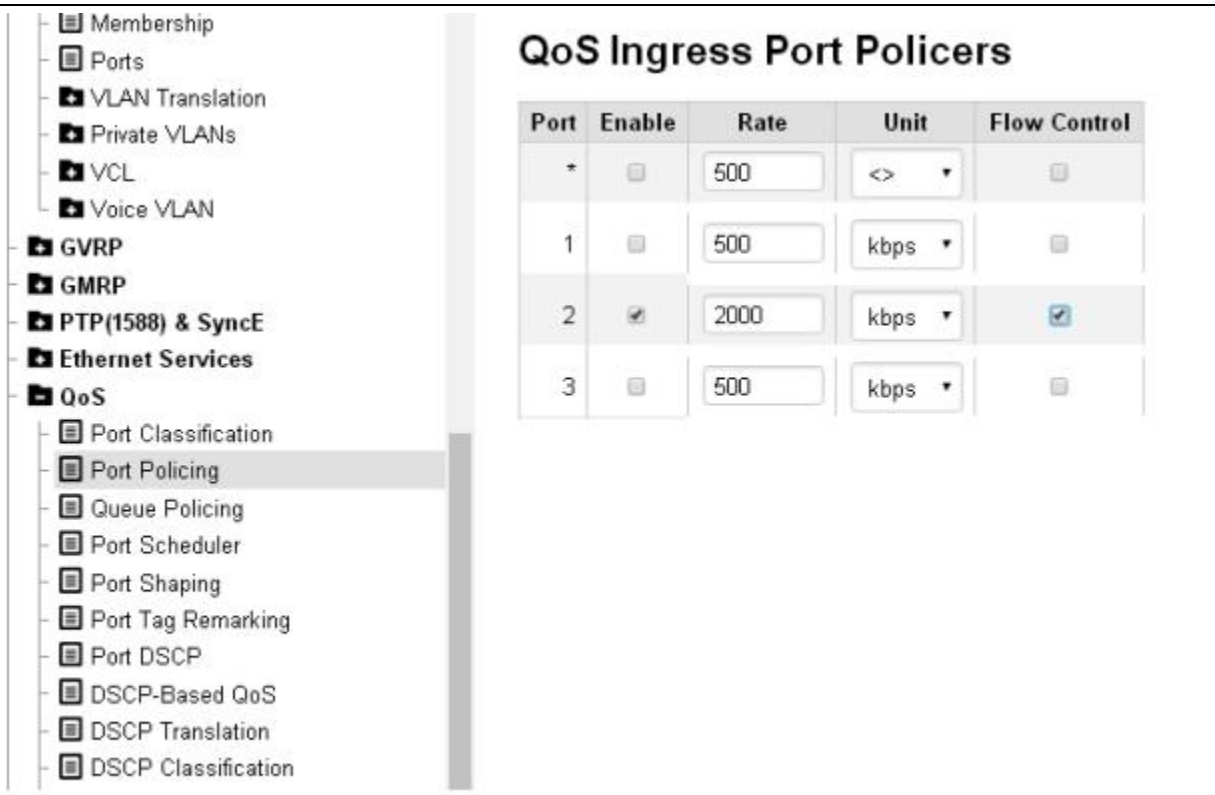

Figure 6-9 QoS ingress port policers

6.3.2.2 Queue Policers

Enables policy on queue 2 of port 2. Set the rate to 20 Mbps

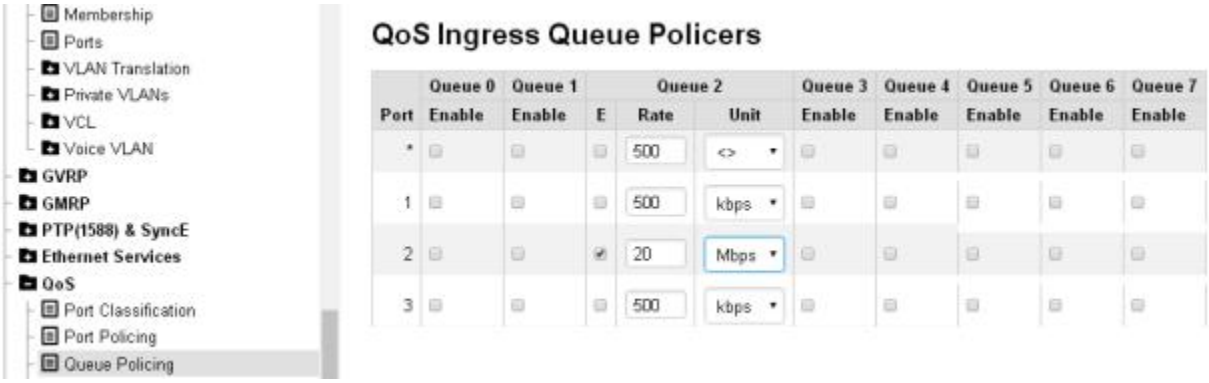

Figure 6-10 QoS ingress queue policers

6.4 Shapers

6.4.1 Port Shapers

Enable Shaper on Port 3 and set the shaper rate to 4000 Kbps, Enable shaping on Queue 2 and Queue 4 on Port 3, showed as the figure 6-12.

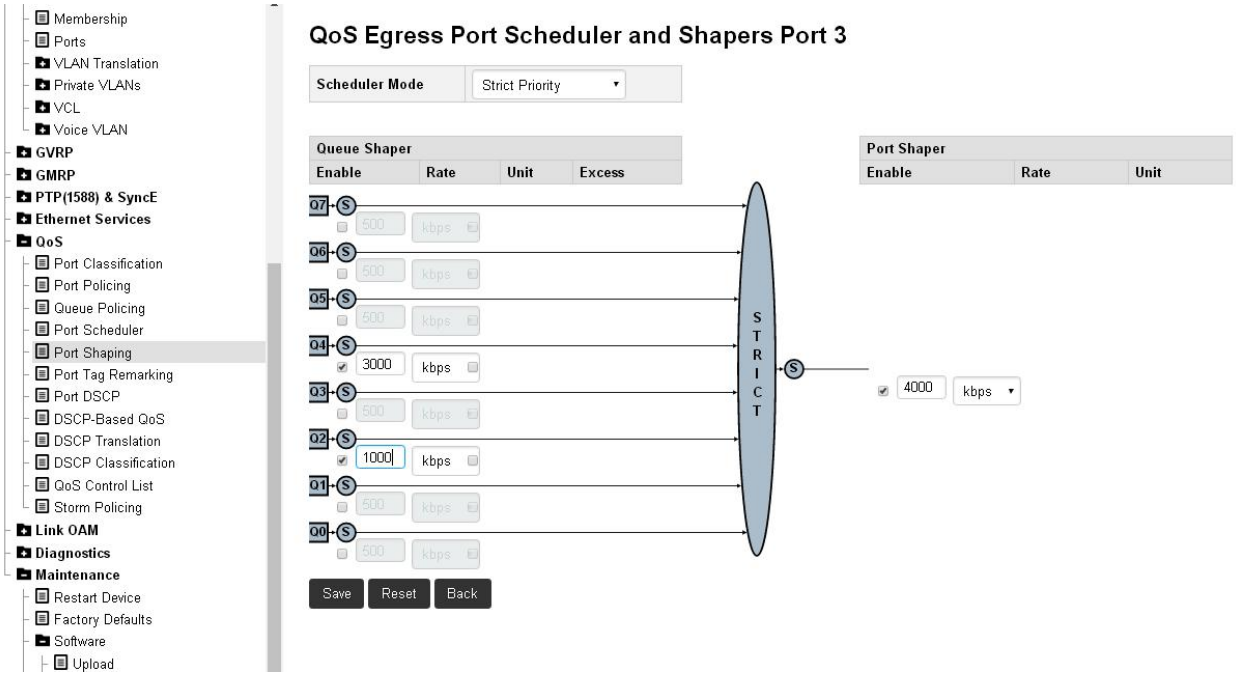

Figure 6-11 shapers port 3

6.5 Schedulers

6.5.1 DWRR

Set the scheduling mode to DWRR on Port 3, the weight setting queue 0 to 40, Queue1 to 40, Queue2 to 20, Queue3 to 20, Queue4 to 20 and Queue5 to 20, showed as the figure 6-12.

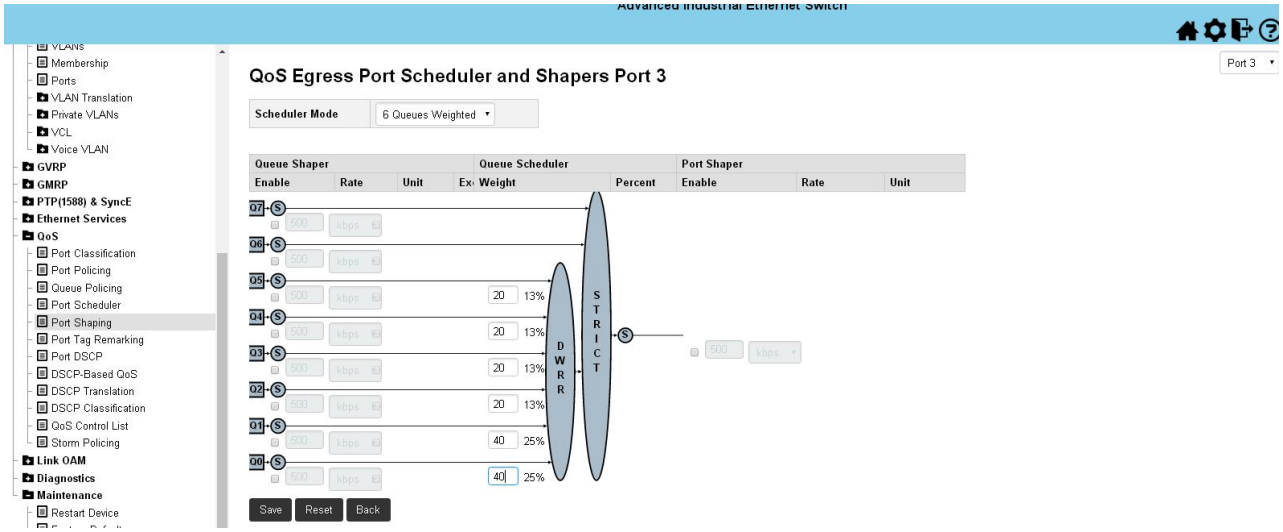

figure 6-12 DWRR on port 3

7 LACP

LACP is the IEEE 802.3ad standard protocol. The link aggregation control protocol allows multiple physical ports to be bundled together to form a single logical port.

7.1 Port based Configuration

Enable/Disable LACP

Control whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the peer device with LACP enabled. Default value is disabled.

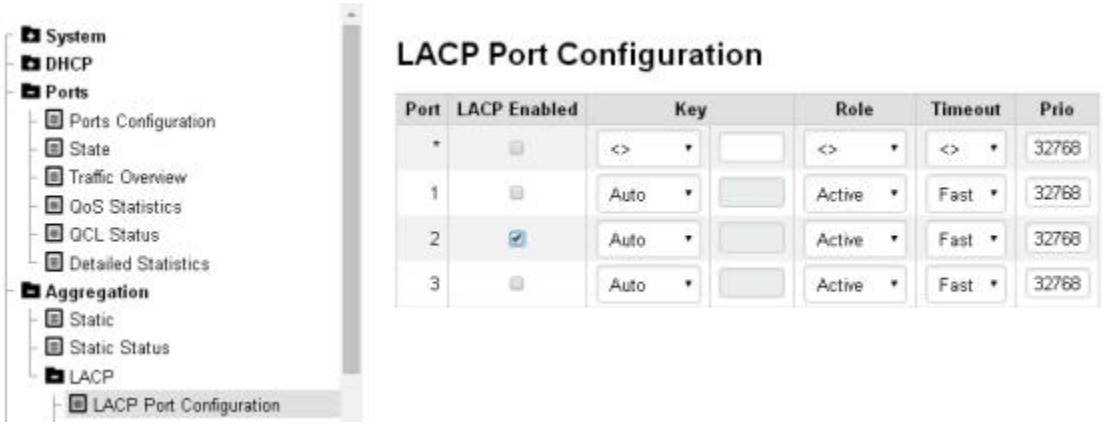

Figure 7-1 LACP enable on port 2

7.2 LACP Key Configuration

The key value range of the port is 1-65535. The automatic setting mode is configured according to the physical link speed (10Mb = 1,100Mb = 2,1Gb = 3). With a specific setting, you can enter a user-defined value. Ports with the same Key value can participate in the same aggregation group, and ports with different key values can not be aggregated. The default value is auto.

Set LACP key to 4 on the port 2, showed as the figure 7-2.

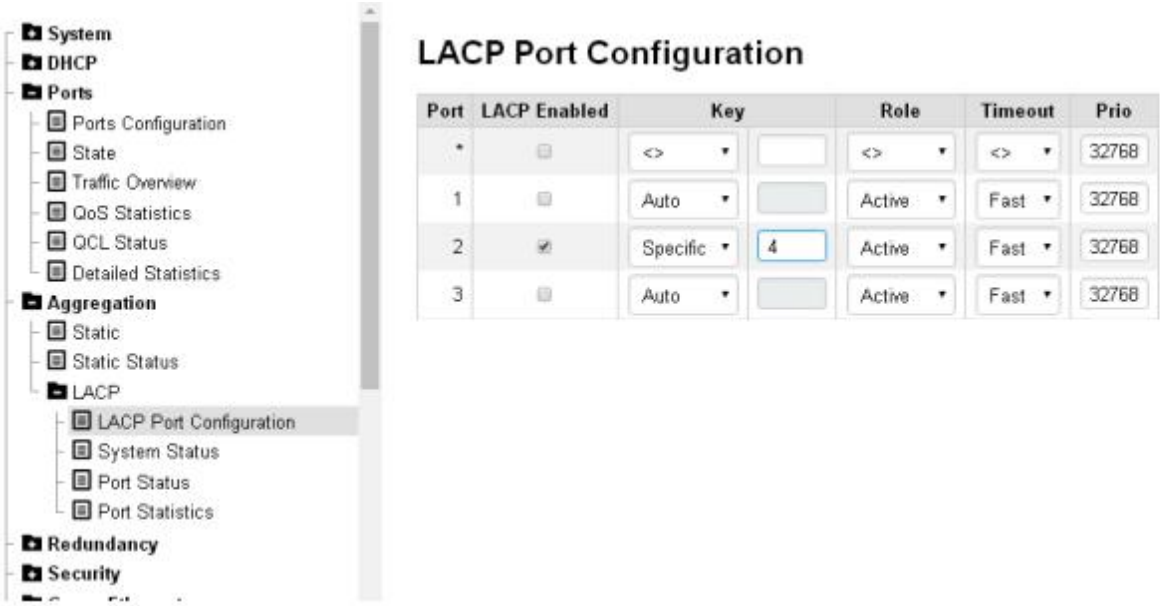

Figure 7-2 Set LACP key to 4 on the port 2

7.2.1 LACP Role Configuration

This role displays the LACP activity status. The Active state sends LACP packets per second, while the Passive state needs to wait for the peer LACP packet. The default value is active.

7.2.2 LACP Timeout Configuration

This configuration controls the time interval between BPDU transmissions. Fast transmits LACP packets per second, while Slow sends LACP packets every 30 seconds. The default value is fast.

8 MAC Address Table

The switching of frames is based on the source MAC address in the frame. The switch creates a table that maps the MAC address to the switch port, which contains static and dynamic MAC addresses. If you want to make a fixed mapping between the DMAC address and the switch port, you need to configure a static MAC.

The switch automatically updates the dynamic MAC address table according to the source MAC address of the frame. If the MAC address is not received after the aging time, the dynamic mac address is removed from the MAC table.

8.1 Set MAC Address Table Aging Time

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is called aging.

Change aging time to 200 seconds, as shown in Figure 8-1.

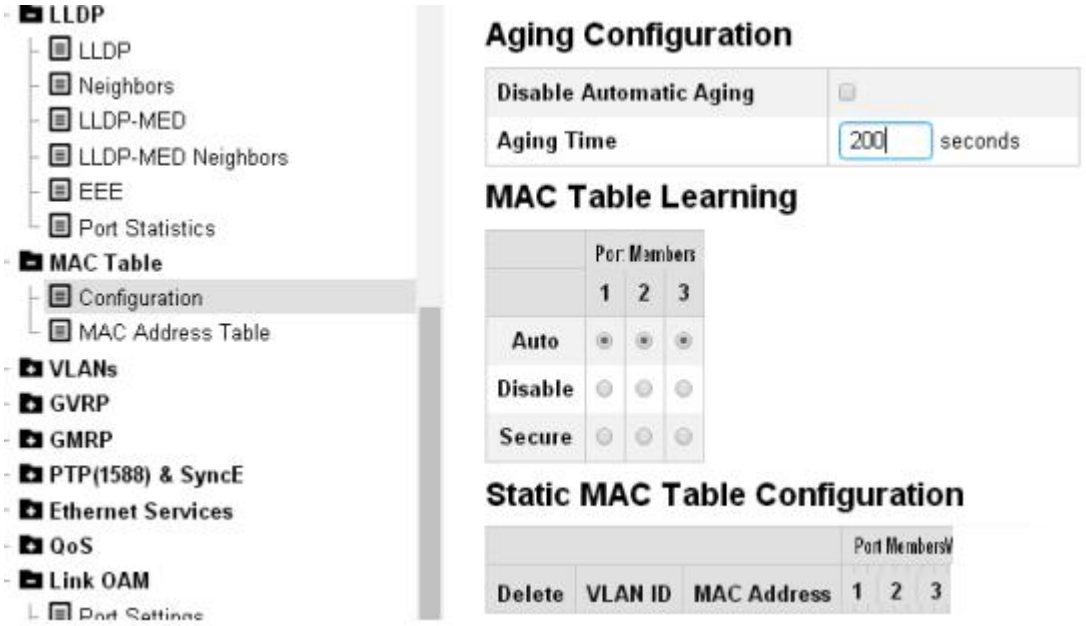

Figure 8-1 Change aging time to 200 seconds

8.2 Add Static MAC Address Table

Add a static MAC address entry to the MAC address table.

Add static MAC address: 00:00:00:00:00:0f to port 3 of VLAN 2. As shown in Figure 8-2.

Figure 8-2 Add static MAC address: 00:00:00:00:00:0f in VLAN 2 on port 3

8.3 Show MAC address table

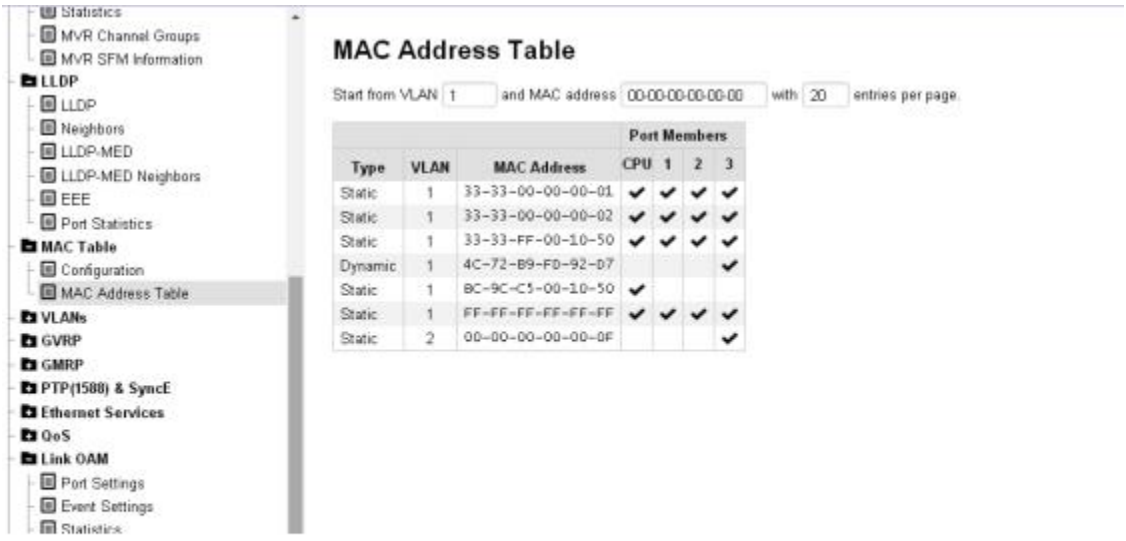

Figure 8-3 Show MAC address table

9 Mirroring & Remote Mirroring

9.1 Mirroring (Local)

To debug network problems or monitor network traffic, the switch system can be configured to mirror frames from multiple ports to a mirrored port.

9.1.1 Type

Mirroring

Configure the switch to local mirror mode. The source port(s) and destination port are located on the same switch.

Source

Configure the switch as a source node of mirroring. The source port(s), reflector port and intermediate port(s) are located on this switch.

Intermediate

As a role of an intermediate transmission to mirroring packets.

Destination

Mirroring packets finally mirrors the destination switch.

9.1.2 VLAN ID

The VLAN ID is the destination VLAN of the mirror. It is recommended to separate from the service VLAN.

9.1.3 Source VLAN(s) Configuration

The switch can support VLAN-based Mirroring.

Note: The Mirroring session shall have either ports or VLANs as sources, but not both.

9.1.4 Port-to-port Mirroring

Mirroring traffic of port 1 to port 3, as shown in Figure 9-1.

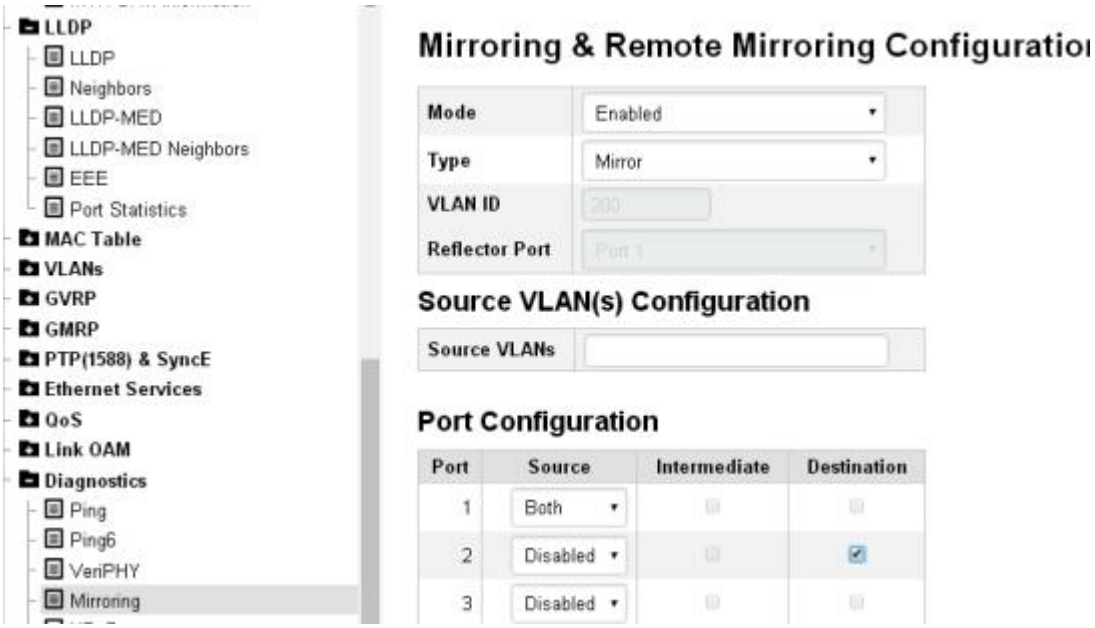

Figure 9-1 Mirroring port 1 traffic to port 6

9.1.5 VLAN to Port Mirroring

Mirroring the traffic of VLAN123 to port 2.

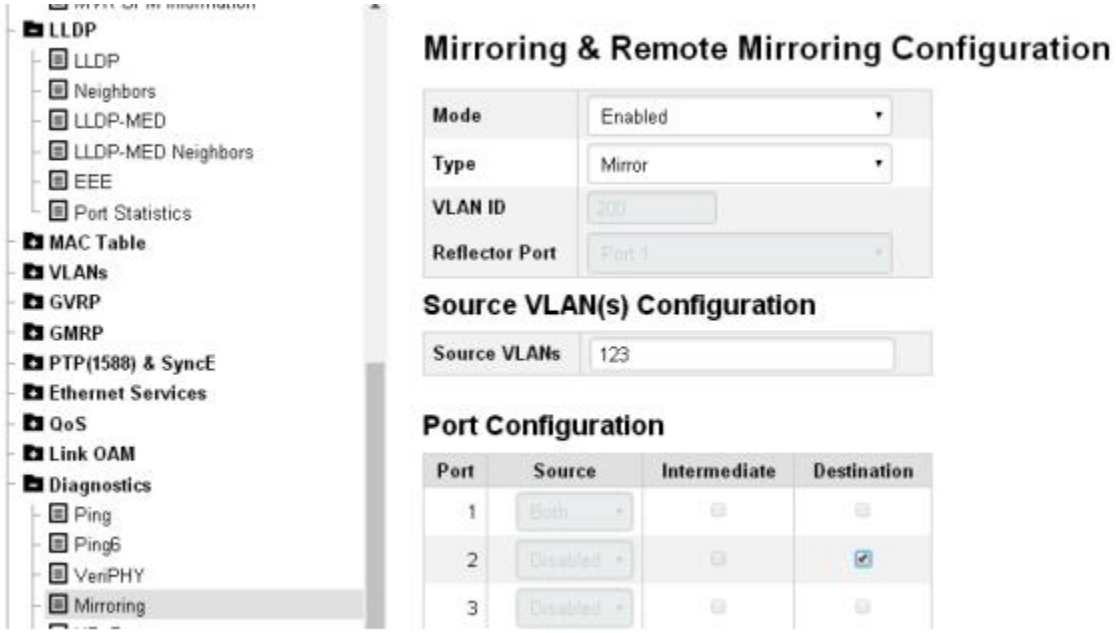

Figure 9-2 VLAN 123 packets are mirrored to port 2

9.2 Remote Mirroring

Remote mirroring is a mirror extension. It can extend the target port in other switches. Enables users to analyze network traffic on other switches.

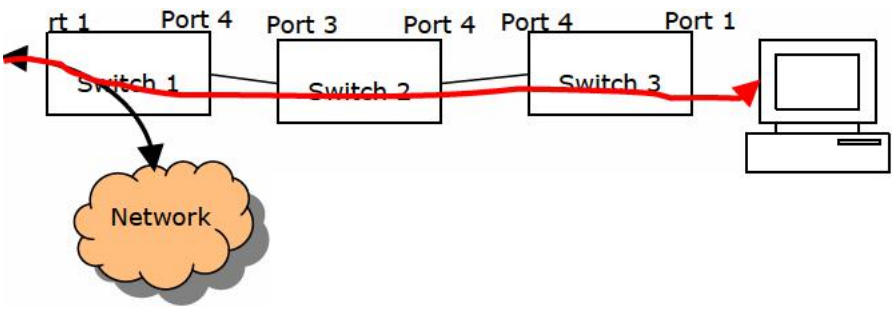

Figure 9-3 Remote mirror topology

Switch 1

Set switch 1 as the source switch with the following parameters

- Source port: 1
- Mirror mode: Both received frames and frames sent will be mirrored.
- Intermediate port: 3

Note: The intermediate port needs to disable MAC table learning.

- Mapping port: 2

Note 1: Mapping ports only need to select the source mirror type.

Note 2: Mapping ports need to disable MAC table learning and STP.

Note 3: The mapping port only supports electrical ports.

- Mirroring VLAN: 200

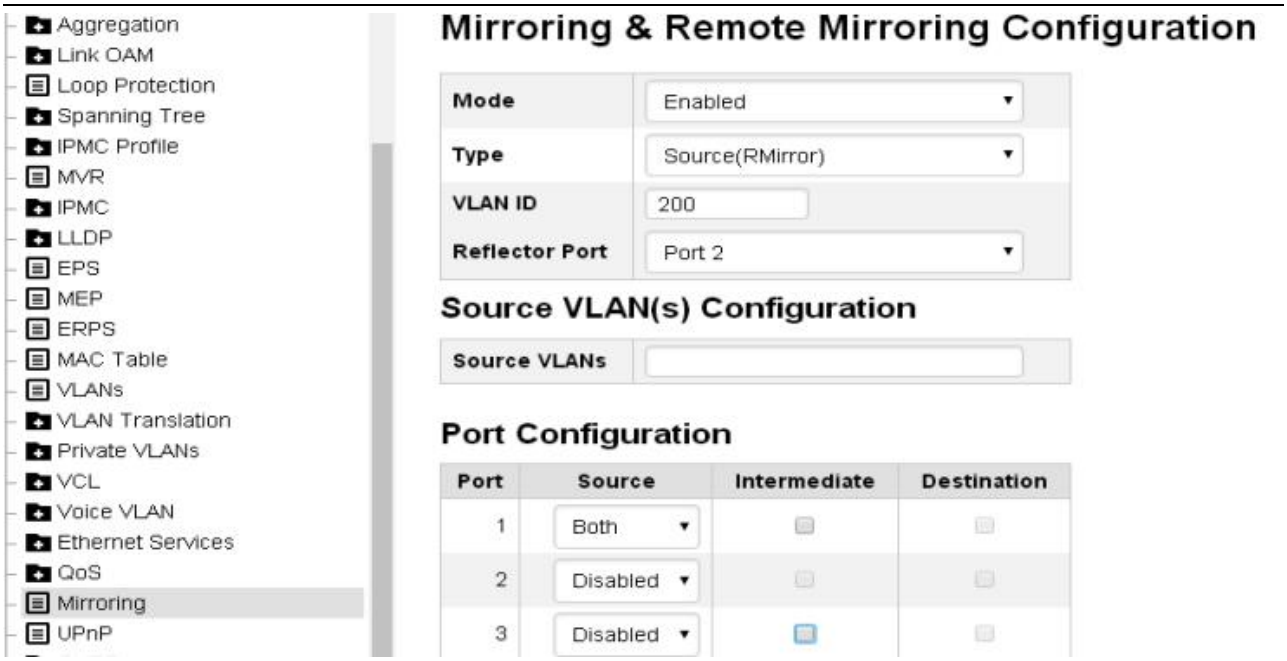

Figure 9-4 Remote mirror - source switch

Switch 2

Use the following parameters to configure Switch 2 as an intermediate switch

Intermediate port: 3. Note: The intermediate port needs to disable the MAC table learning.

Mirror traffic VLAN: 200

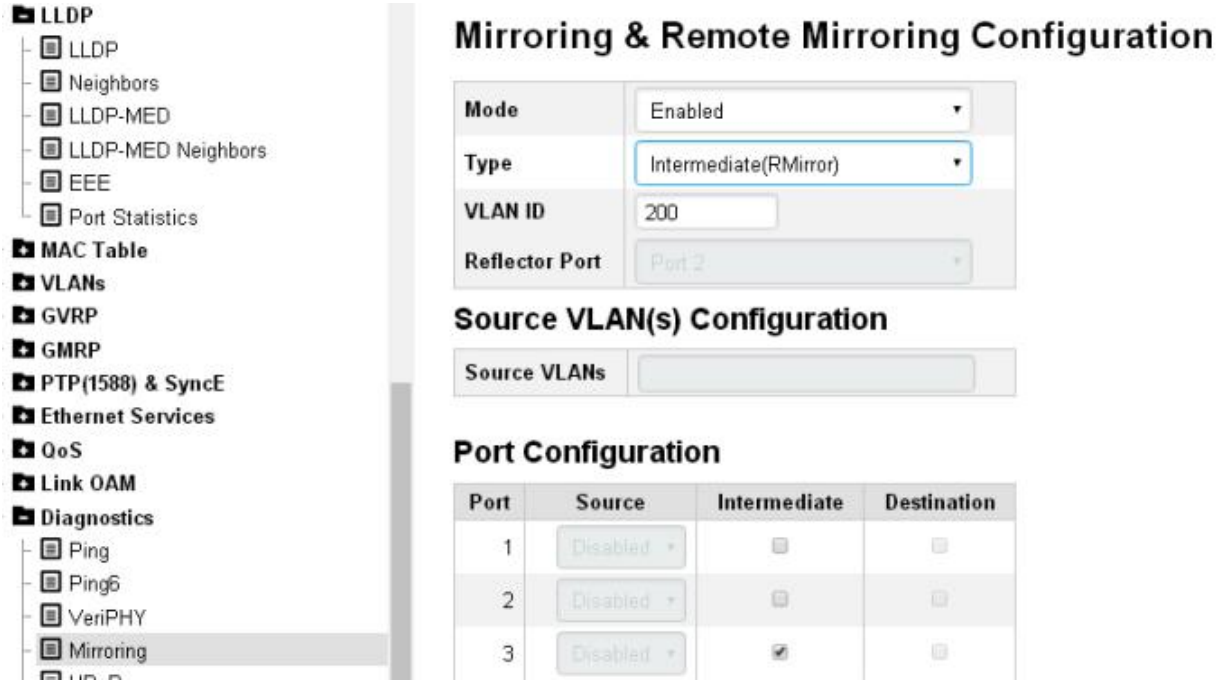

Figure 9-5 Remote mirroring intermediate switch configuration

Switch 3

Use the following parameters to configure Switch 3 as the destination switch

Intermediate port: 3

Note: The intermediate port needs to disable MAC table learning.

Destination port: 1

Note 1: The device supports only one destination port.

Note 2: The destination port needs to disable MAC table learning.

Mirror traffic VLAN: 200

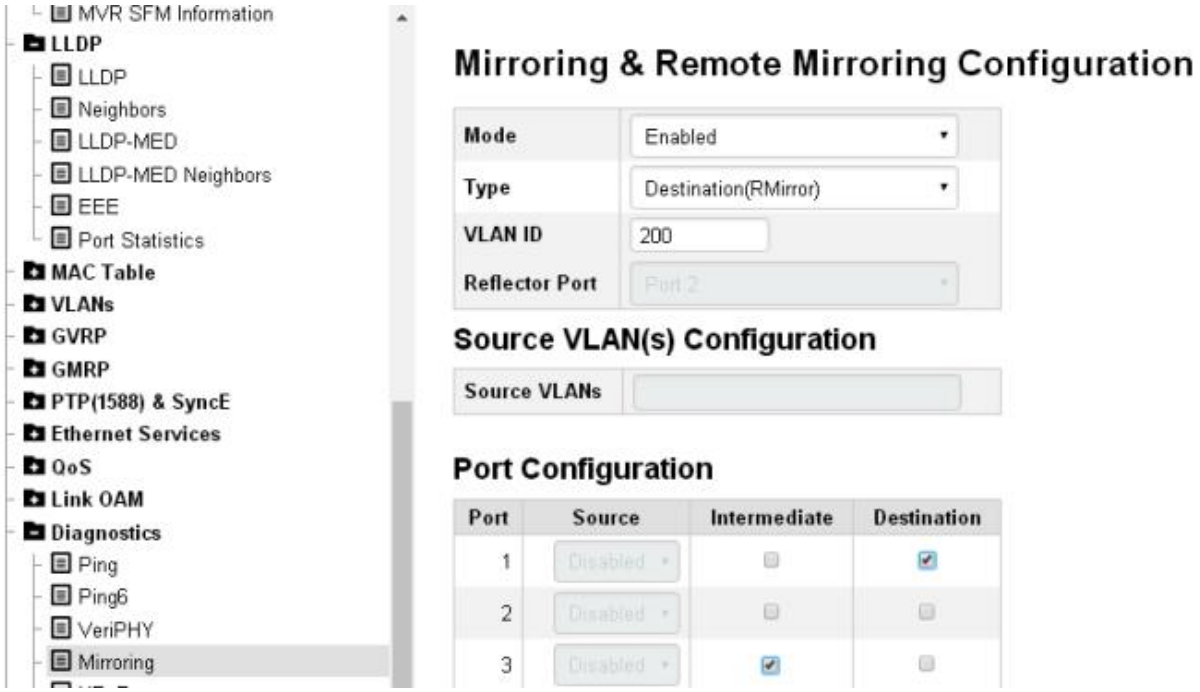

Figure 9-6 Remote mirroring destination switch

10 GVRP

Generic VLAN Registration Protocol or GVRP, IEEE 802.1Q-2005, clause 11 and IEEE 802.1D -2004, clause 12.

10.1 GVRP Port Configuration

GVRP port is showed as below.

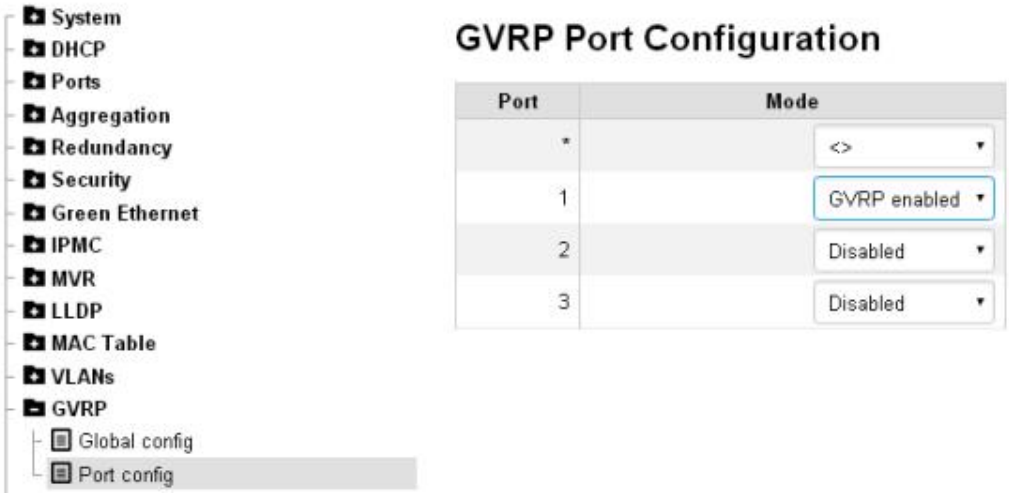

Figure 10-1 GVRP enable

10.2 GVRP Global configuration

A small number of parameters can be configured for GVRP. These parameters are in the web config shown below.

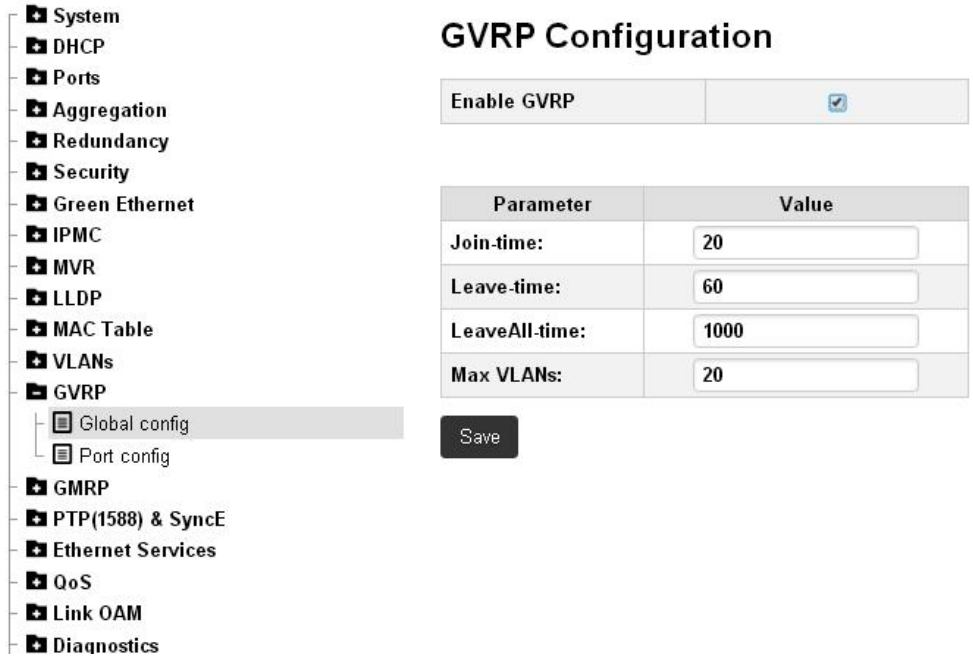

Figure 10-2 GVRP configuration

11 Multiple Spanning Tree Protocol(MSTP)

11.1 Bridge Configuration

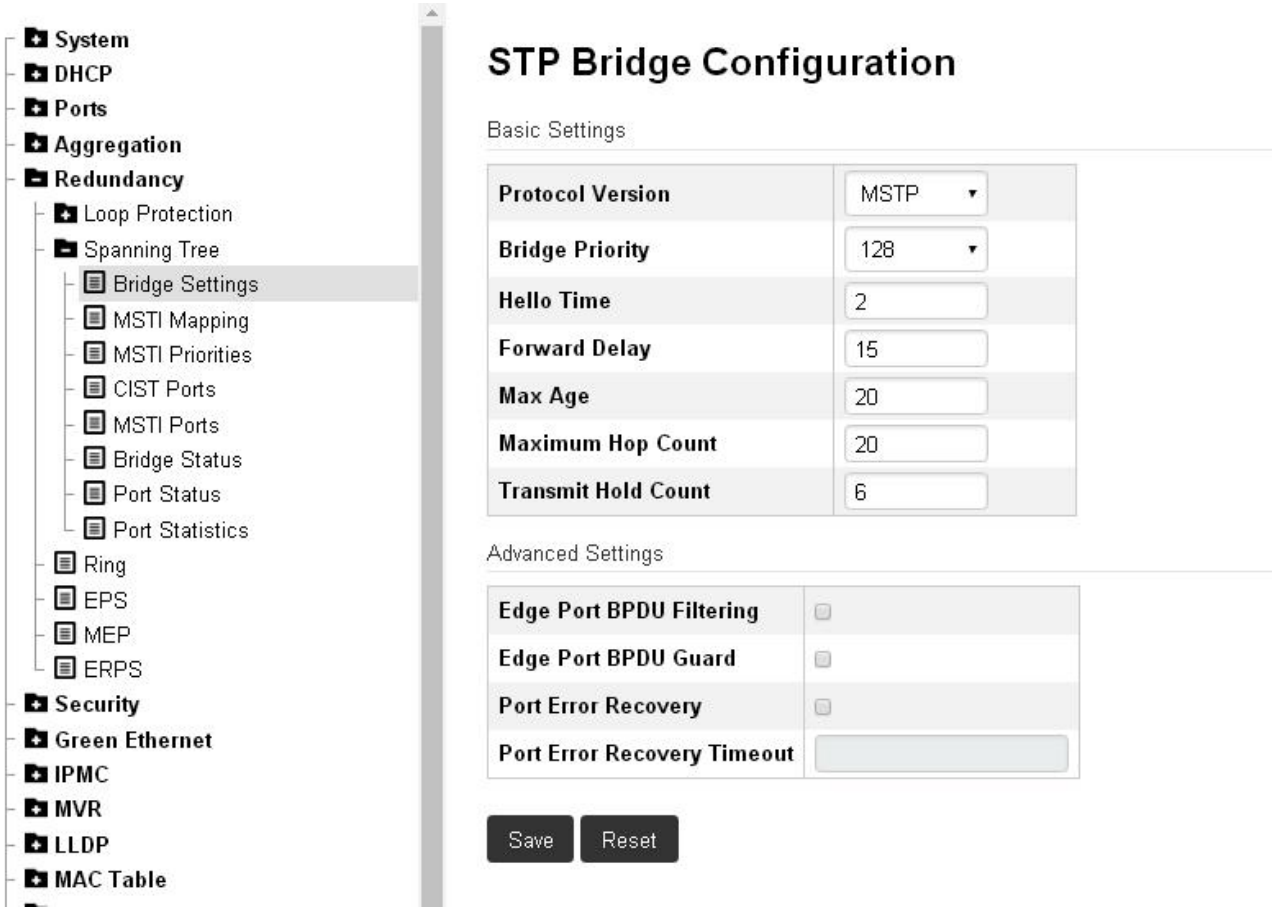

Figure 11-1 STP Bridge Configuration

11.2 MSTI Configuration

By default, all VLAN IDs are mapped to CIST. If the protocol type is set to MSTP, the VLAN ID can be mapped to one of the eight spanning trees, where CIST is 1. The other seven are called MSTI1, ..., MSTI7, as shown. The MSTI configuration also has a name and a version, as shown in the figure. All of these values must be configured on the same switch in the network, otherwise the configuration will not take effect.

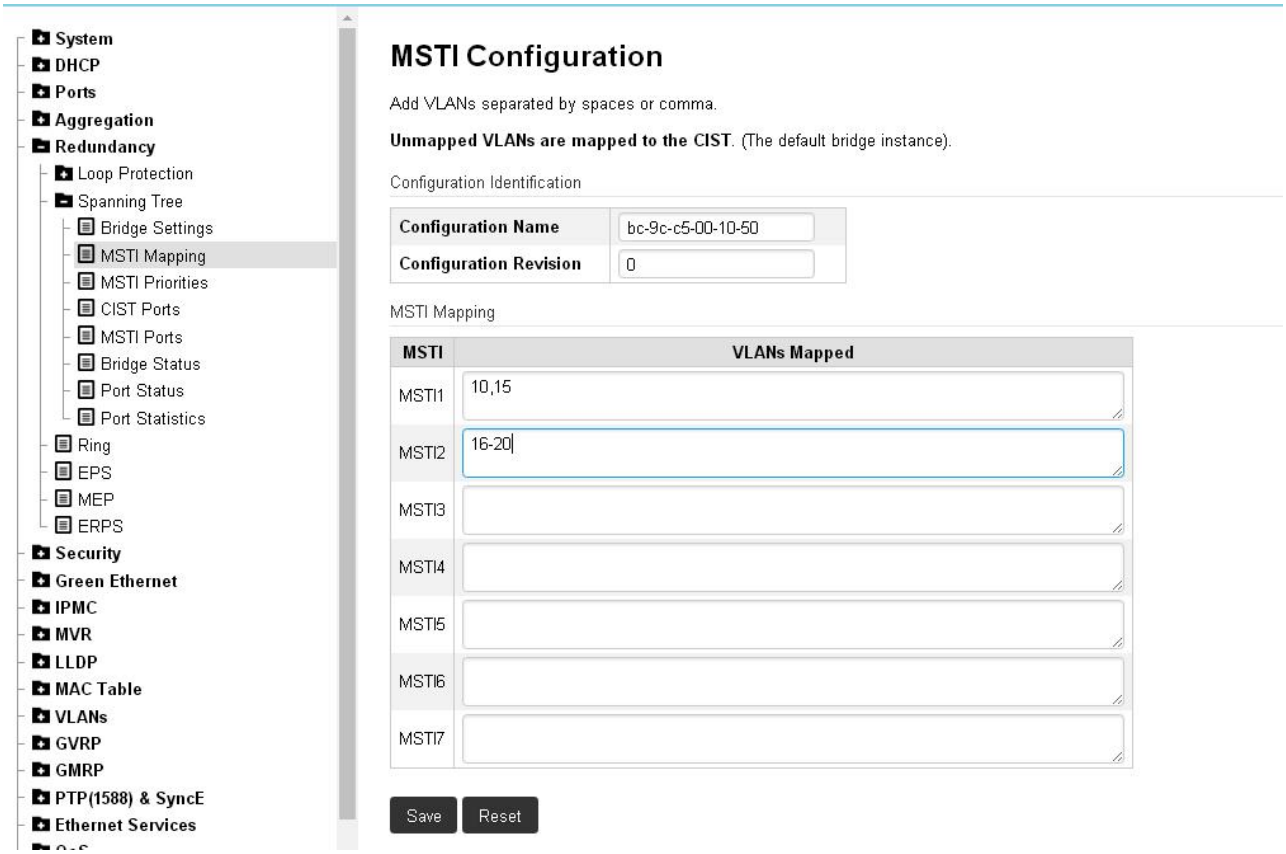

Figure 11-2 MSTI configuration

11.3 MSTI Priorities

Each MSTI and CIST can be given a priority as show below.

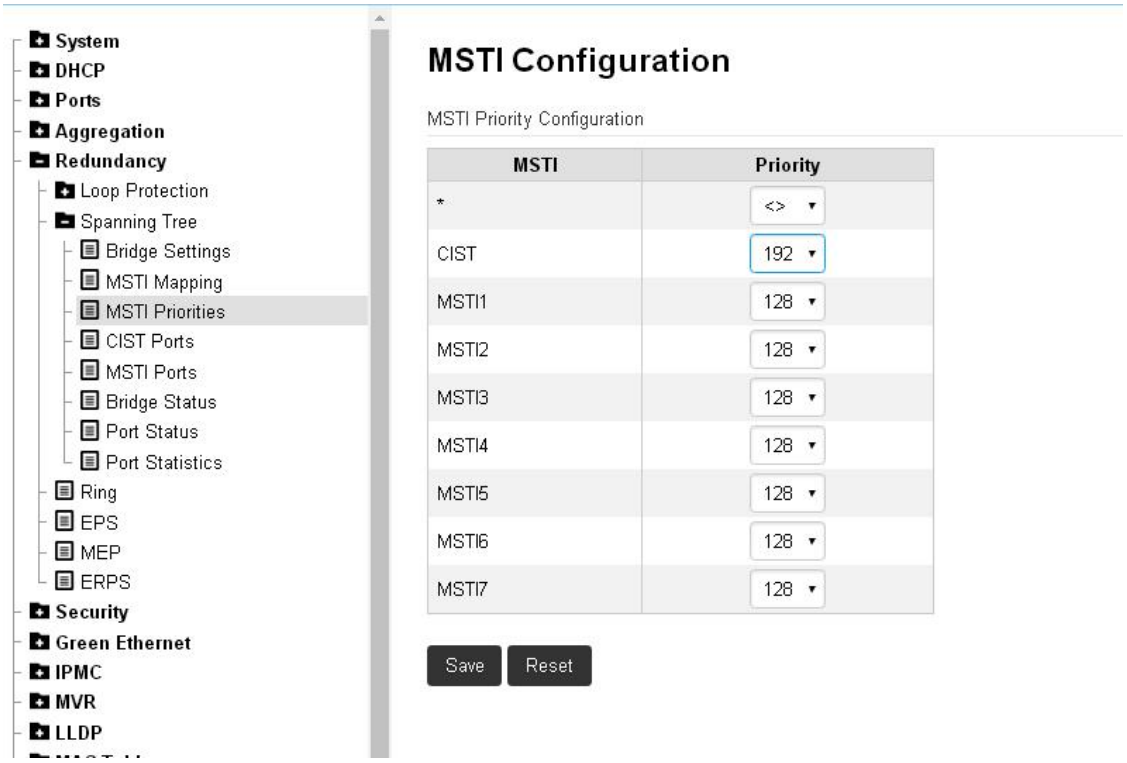

Figure 11-3 **MSTI attributes**

A low priority number means higher priority. A Bridge Identifier is constructed per CIST, MSTI1,…,MSTI7, which is the Bridge Priority, see Figure 11-3, plus the number in the figure above. This is concatenated with the MAC address of the switch. In this way the Bridge Identifier should be unique.

A low Bridge Identifier means higher priority. A high priority means that the switch tends to be the root of the spanning tree in favor of switched with lower priority. So if two switched has the same Bridge Priority, then by e.g. selecting MSTI1 priority higher on the one switch than the other, and vice versa with MSTI2, the one switch tends to be root of the one MSTI and the other switch for the other MSTI.

11.4 STP CIST port configuration

Configure port-based STPs in the Web, as shown in Figure 11-4.

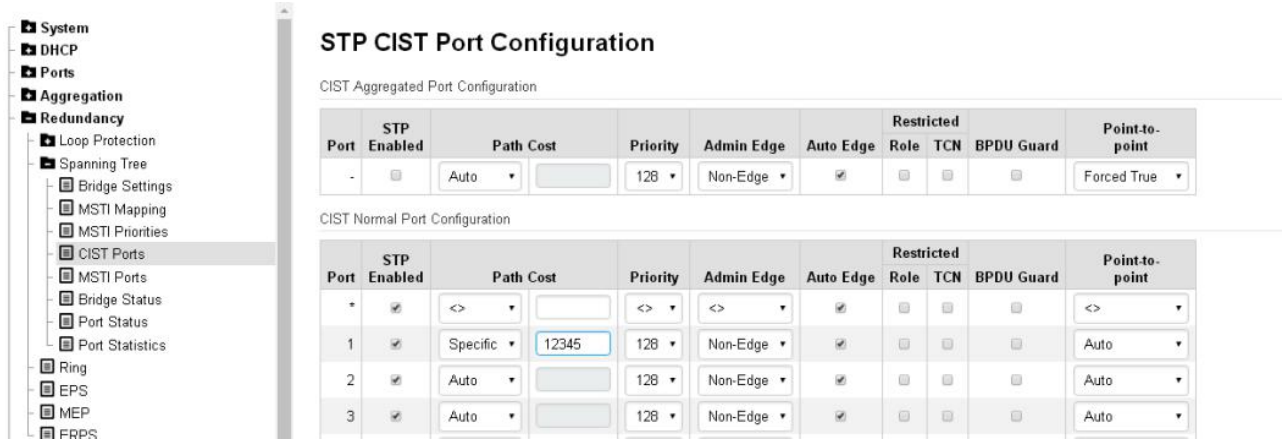

Figure 11-4 **CIST port configuration**

Let's start with pointing out, that all parameters above(except Path Cost and Priority) are specific for the port and not for CIST. Also there is a CIST Aggregation Port Configuration and a CIST Normal Port Configuration. All the configurations done in the second case is done in the Config Interface mode.

11.4.1 Edge port

The edge port is the port that is not connected to the bridge. If auto edge is enabled, then the port determine whether a port is an edge port by registering if BPDUs are received on that port. The admin edge determines what the port should start as being – edge or not, until auto edge – if enabled, change it.

The final result can be seen by selecting Monitor>Spanning Tree>Bridge Status, then clicking on CIST. Then the field Edge shows the decision.

11.4.2 Restricted Role and Restricted TCN

If restricted role is enabled, it causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it may cause lack of spanning tree redundancy. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard. If restricted TCN is enabled, it causes the port not to propagate received topology change notifications and topology changes to other ports.

11.4.3 BPDU Guard

If enabled, it causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not affect this setting.

11.4.4 Point-to-point

Where the no form is equivalent to setting it to auto.

Setting the link to point-to-point, shows up in the web interface as Forced True. Setting it to shared, is shown as Force False. Setting it to auto shows as Auto.

11.5 MSTI Port Configuration

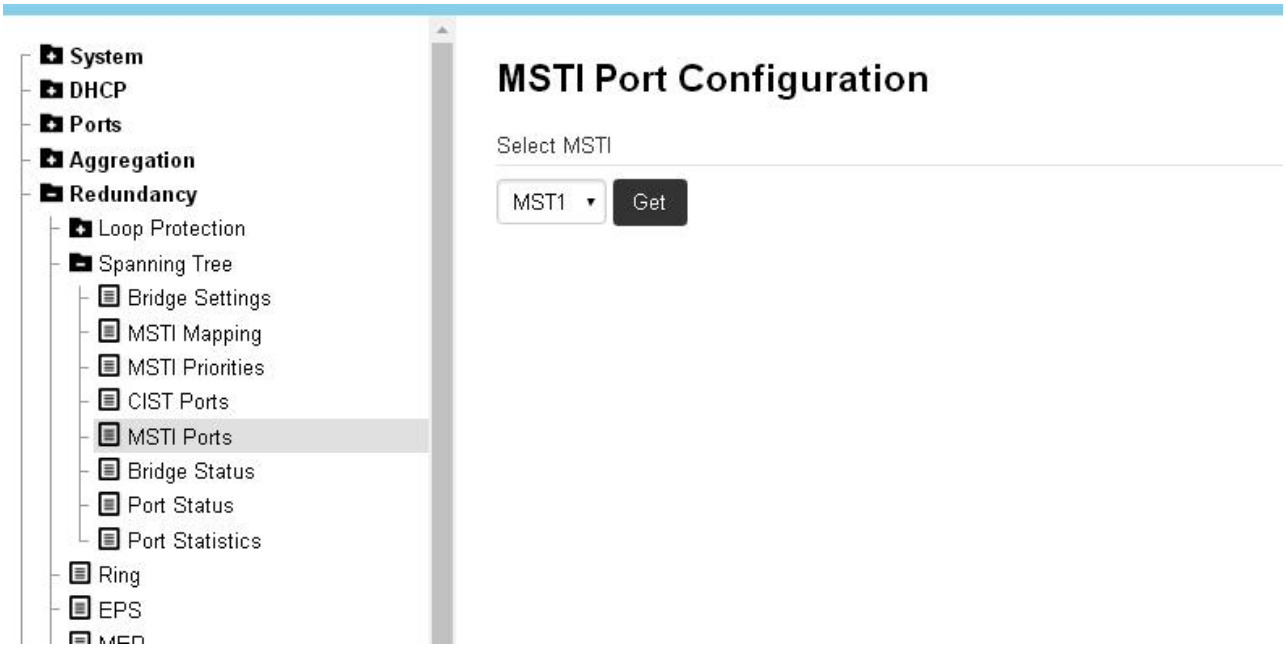

Figure 11-5 MSTI port configuration

Then select the MSTI wanted, and press get.

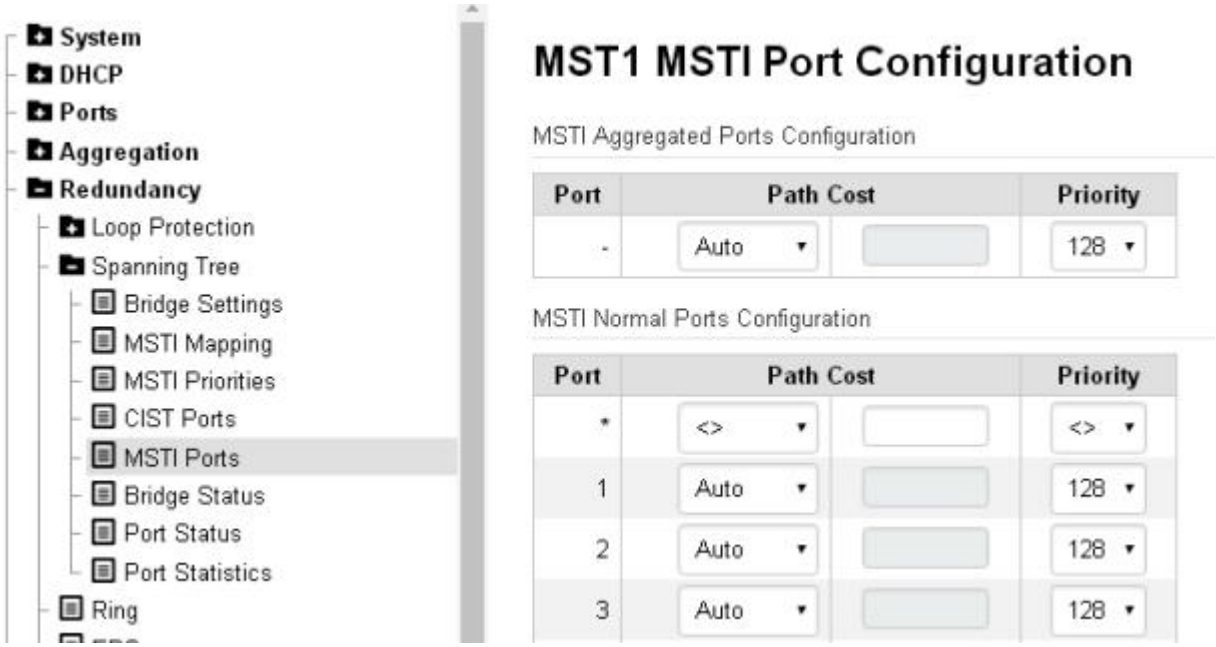

Figure 11-6 MSTI port configuration

The <Cost> is a number in the range 1,…,200000000 or it may be auto. If set to auto, then the path cost will be set to the value appropriate for the physical link speed, using IEEE 802.1D recommended values.

The <Priority> is a number in the range 0,…,240 and a multiple of 16. Note it is not a multiple of 16 then it will be set to 0.

The path cost is used by STP when selecting ports. Low cost is chosen in favor of high cost. And if two ports have the same cost, then priority is used as a tie breaker.

12 Ethernet Ring Protection Switching(ERPS)

ERPS ID

The ID of the created Protection group, It must be an integer value between 1 and 64. The maximum number of ERPS Protection Groups that can be created are 64. Click on the ID of an Protection group to enter the configuration page.

Port 0

This will create a Port 0 of the switch in the ring.

Port 1

This will create "Port 1" of the switch in the Ring.

Ring Type

Type of Protecting ring. It can be either major ring or sub-ring.

Alarm

ERPS alarm

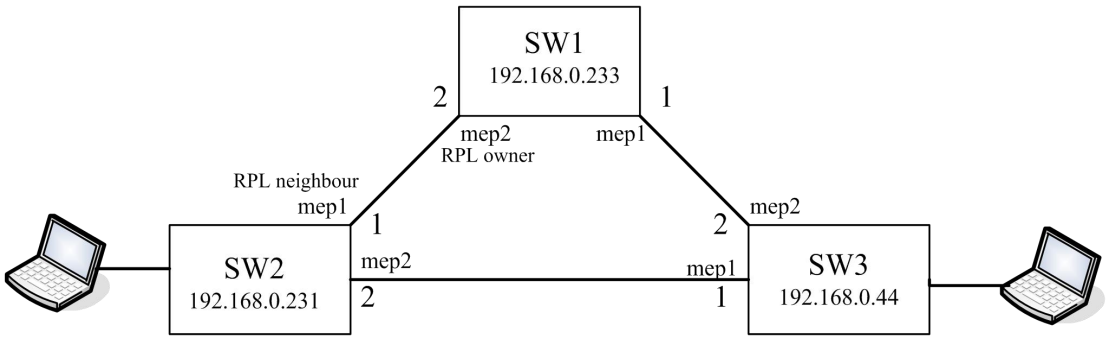

Figure 12-1 network connection topology

1. Connect Swtich 1 and Switch 2, switch 2 and Switch 3. Do not connect switch 1 and 3 to avoid ringing.

2. Restore the default value of switch 1/2/3. Disable the DHCP client and set the correct static IP for switch 1/2/3.

In this example, switch 1 is 192.168.0.233, switch 2 is 192.168.0.231, switch 3 is 192.168.0.44.

3. On switch 1/2/3, disable spanning tree (which is enabled in the default settings) to avoid conflicts with ERPS.

4. Enable Vlan tag awareness on switch 1/2/3. (Set the port type port C of port 1 and port 2 of switch1/2/3).

5. ERPS

5.1 Swtich 1 RPL Owner

Figure 12-2 Add ERPS on switch 1

Edit ERPS (by clicking “1” under ERPS ID ERPS table)

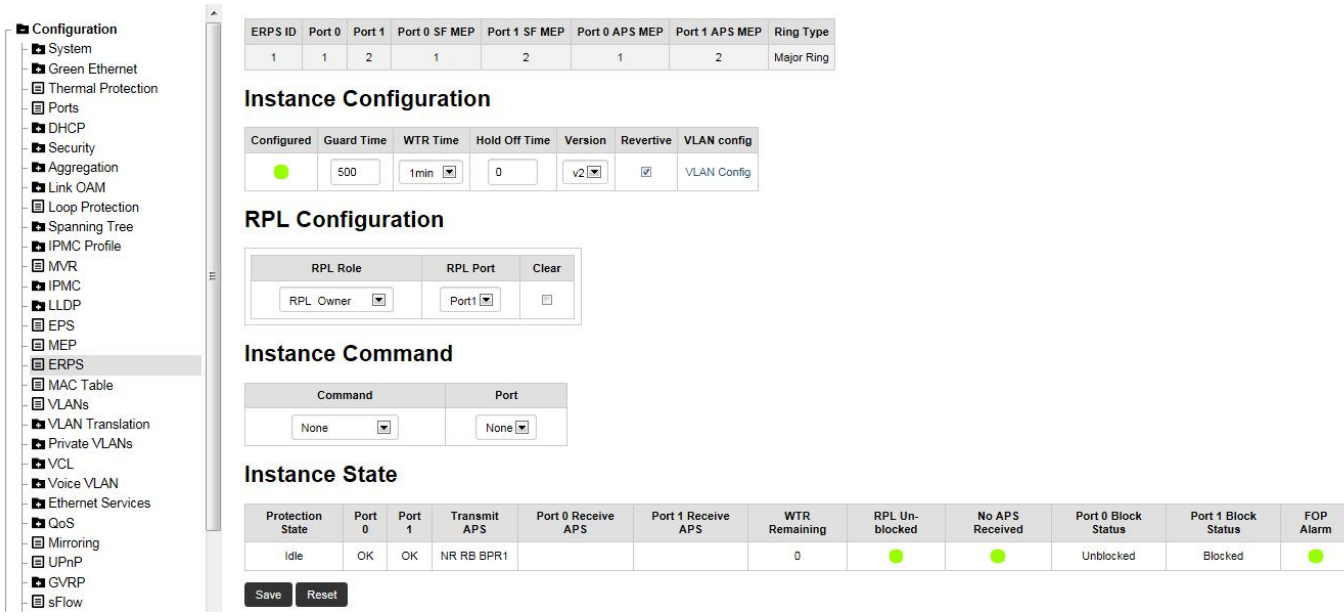

Figure 12-3 Edit ERPS

Edit protected VLANs

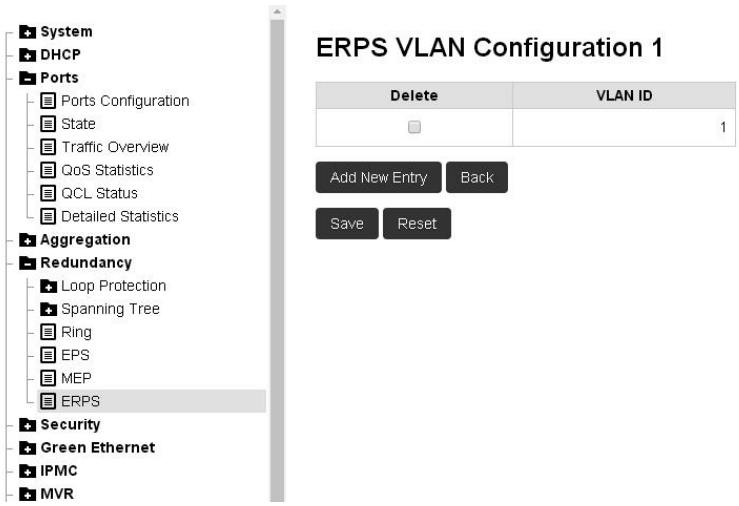

Figure 12-4 Protected VLANs

5.2 Switch 2, RPL neighbor

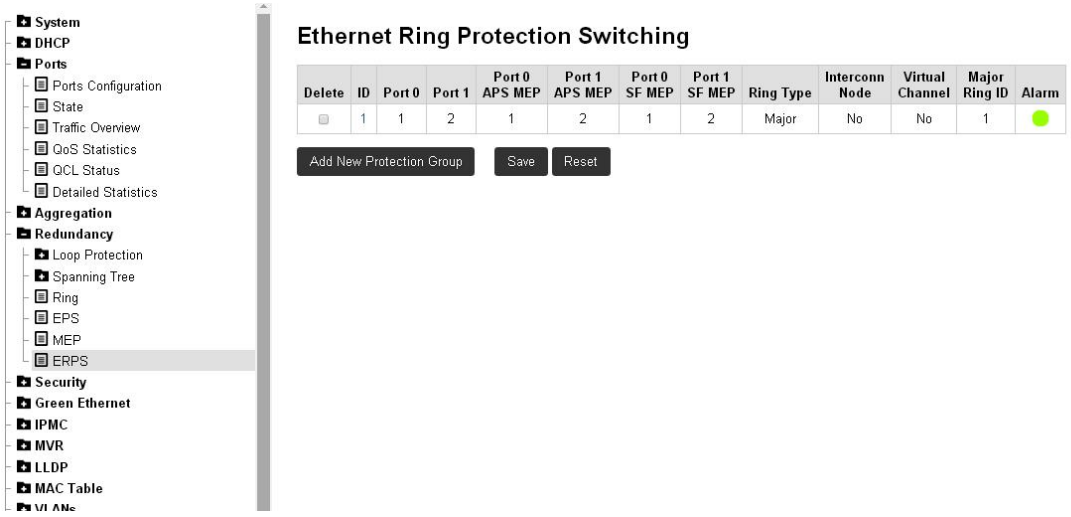

Figure 12-5 Add ERPS on switch 2

Edit ERPS1 (by clicking “1” under ERPS ID ERPS table)

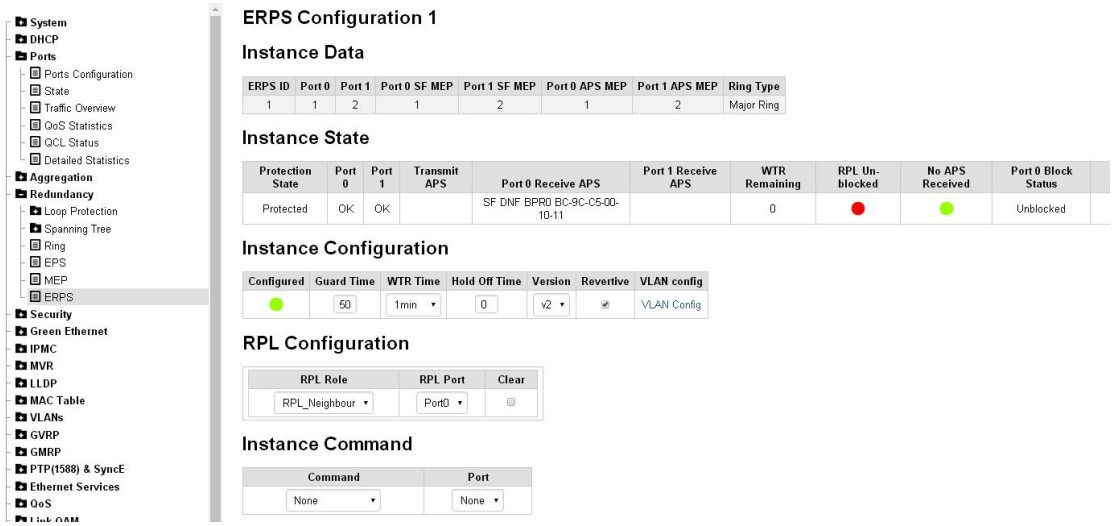

Figure 12-6 Edit ERPS

Edit protected VLANs

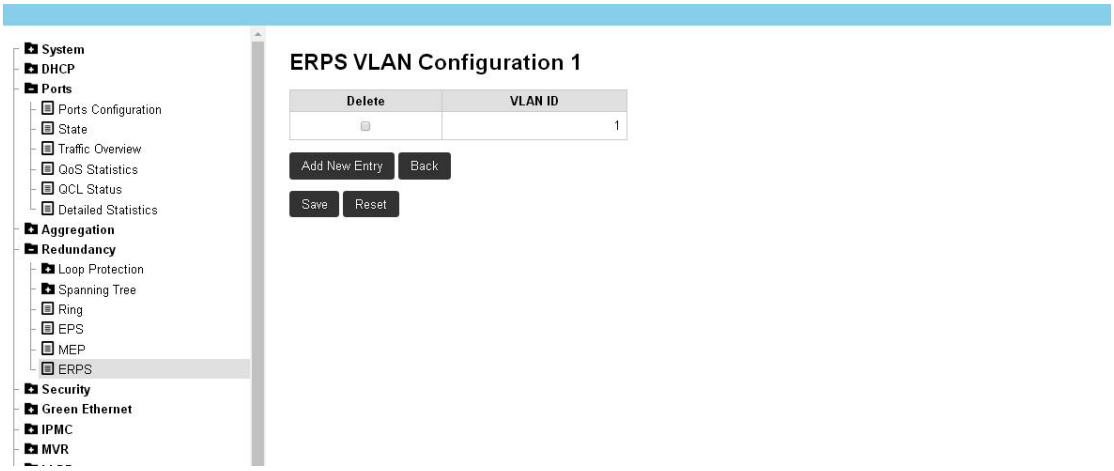

Figure 12-7 Protectd VLANs

5.3 Switch 3

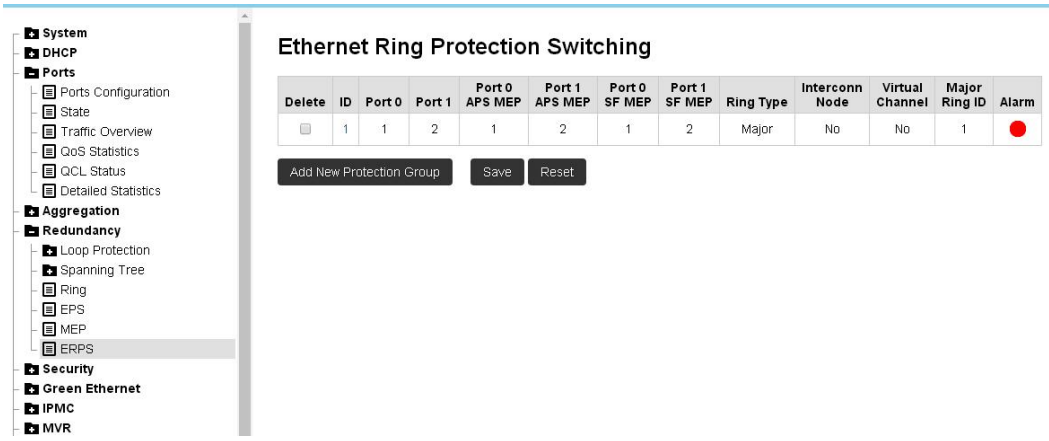

Figure 12-8 Add ERPS on switch 3

Edit ERPS1 (by clicking “1” under ERPS ID ERPS table)

Edit protected VLANs

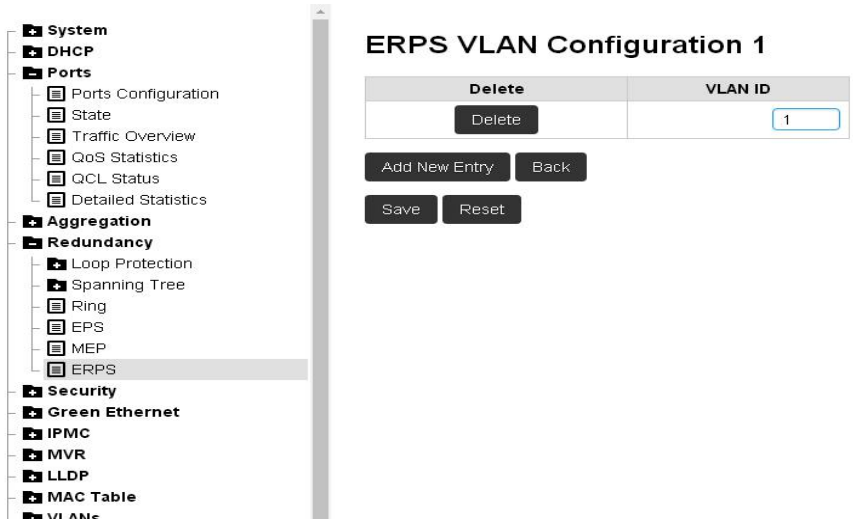

Figure 12-9 Protected VLANs

6. Connect switch 1 and switch 3, and check whether MEP of 3 switches are normal.

Switch 1

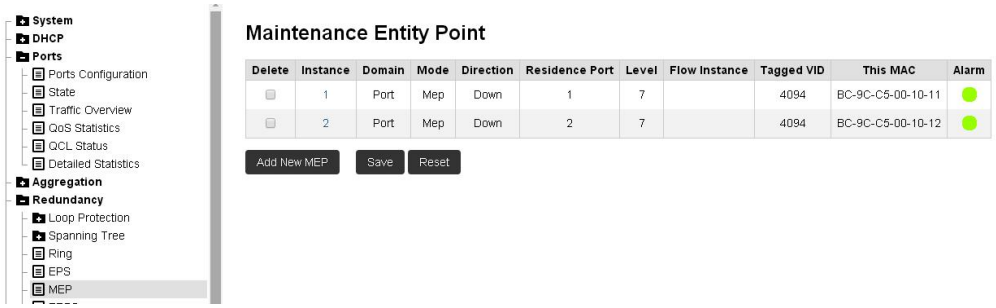

Figure 12-10 MEP of switch 1

Switch 2

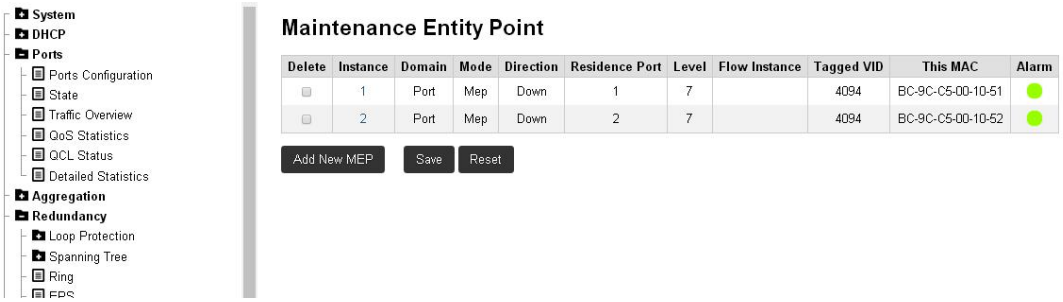

Figure 12-11 MEP of switch 2

Switch 3

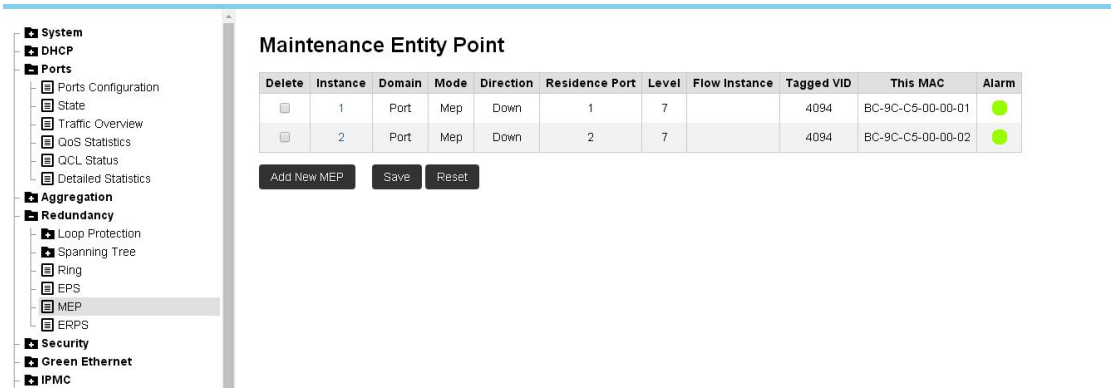

Figure 12-12 MEP of switch 3