FSM-510G series

10-Port Managed Industrial Ethernet Switch

User Guide

Version Number:
Issue: 1.0, Dec 2014

[CONTENTS]

[LIST OF TABLES]

[LIST OF FIGURES]

Preface

Scope

Audience

Safety Instructions

Documentation Conventions

Preface

Scope

This document provides an overview on FSM-510G. It contains:

- Descriptive material about the FSM-510G Hardware Installation Guide.

Audience

The guide is intended for system engineers or operating personnel who want to have a basic understanding of FSM-510G.

Safety Instructions

When a connector is removed during installation, testing, or servicing, or when an energized fiber is broken, a risk of ocular exposure to optical energy that may be potentially hazardous occurs, depending on the laser output power.

The primary hazards of exposure to laser radiation from an optical-fiber communication system are:

- Damage to the eye by accidental exposure to a beam emitted by a laser source.
- Damage to the eye from viewing a connector attached to a broken fiber or an energized fiber.

Documentation Conventions

The following conventions are used in this manual to emphasize information that will be of interest to the reader.

Danger — The described activity or situation might or will cause *personal injury*.

Warning — The described activity or situation might or will cause *equipment damage*.

Caution — The described activity or situation might or will cause *service interruption*.

Note — The information supplements the text or highlights important points.

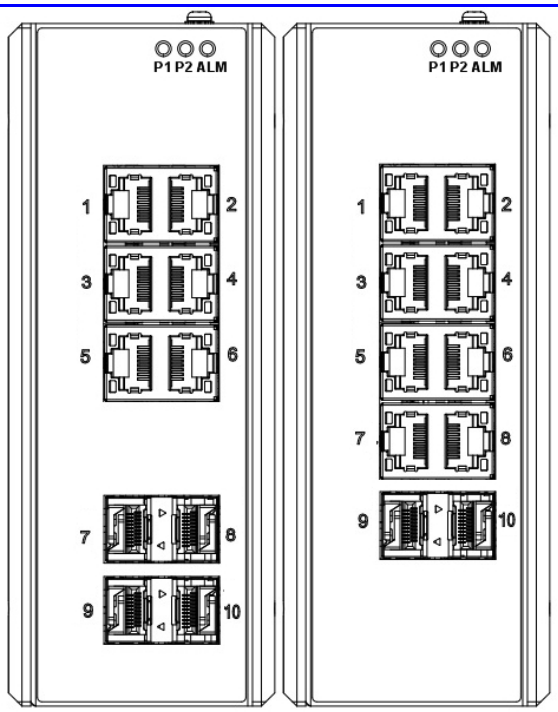
Overview

Overview

FSM-510G series industrial Ethernet solutions deliver high quality, wide operation temperature range, extended power input range and advanced VLAN & QoS features. It's ideal for harsh environments and mission critical applications.

Faceplate

10-Port series



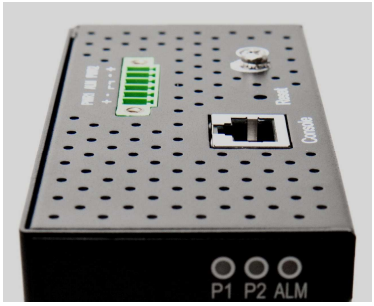
Front Panel Introduction

Front Panel	
System Status LED	P1, P2 and Alarm
Gigabit Ethernet Copper Ports	RJ45
Gigabit Ethernet SFP ports	SFP Slots

Models	L2+ Managed Switch	
	FSM-510G-2F	FSM-510G-4F
Total Gigabit Ethernet Ports	10	10
10/100/1000 BaseT(X)	8	6
100/1000 Base SFP	2	4

Top Panel Introduction

Top Panel	
Power Input (Dual)	6P Terminal Block
Console (RS232)	RJ45
Reset	Push Button



Technical Specifications

Ethernet	
Operating mode	Store and forward, L2 wire-speed/non-blocking switching engine
MAC addresses	8K
Jumbo frames	9K Bytes
Copper RJ45 Ports	
Speed	10/100/1000 Mbps
MDI/MDIX Auto-crossover	Support straight or cross wired cables
Auto-negotiating	10/100/1000 Mbps speed auto-negotiation; Full and half duplex
Ethernet isolation	1500 VRMS 1 minute
SFP (pluggable) Ports	
Port types supported	SFP (pluggable) Ports 100/1000Base SFP slot Support 100/1000BaseT SFP transceiver
Fiber port connector	LC typically for fiber (depends on module)
Optimal fiber cable	Typical 50 or 62.5/125 µm for multimode (mm); Typical 8 or 9/125 µm for single mode (sm)
Network Redundancy	
Fast failover protection rings	Link loss recovery < 20ms Single & Multiple rings supported
Spanning Tree Protocol	IEEE 802.1D STP, IEEE 802.1w RSTP, IEEE 802.1s MSTP
Port Trunk with LACP	Static trunk or Dynamic via LACP (Link Aggregation Control Protocol)
Bridge, VLANs & Protocols	
Flow control	IEEE 802.3x (Full Duplex) and Back-Pressure(Half Duplex)
VLAN Types	Port-based VLANs IEEE 802.1Q tag-based VLANs IEEE 802.1ad Double Tagging (Q in Q)
Multicast protocols	IGMP v1, v2 IGMP snooping and querying Immediate leave and leave proxy Throttling and filtering
LLDP	IEEE 802.1ab Link layer Discovery Protocol (LLDP)
Traffic management & QoS	
Priority	IEEE 802.1p QoS
Number of queues per port	8
Scheduling schemes	SPQ, WRR
Traffic Shaper	port-based shaping
Security	
Port security	IP and MAC-based access control IEEE 802.1X authentication Network Access Control
Storm Control	Multicast/Broadcast/Flooding Storm Control

Power	
Power input	Redundant Input Terminals
Input voltage range	12-58 VDC
Max. power consumption	10.5W
Reverse power protection	Yes

Indicators	
Power Status indication	Indication of power input status
Ethernet port indication	Link & Speed

Management	
User Management interfaces	CLI (command line interface) WEB-based Management SNMP v1, v2c Telnet (5 sessions)
Management Security	HTTPs, SSH Radius Client for Management
Upgrade & Restore	Configuration Import/Export Firmware Upgrade
Diagnostic	Syslog Per VLAN mirroring SFP with DDM (Digital Diagnostic Monitoring)
MIBs	RMON 1,2,3,9; Q-Bridge MIB, RFC 1213 MIB-II, RFC 4188 Bridge MIB
DHCP	Client, Server, Relay, Snooping, Option 82
NTP/SNTP	Yes

Environmental & Compliances	
Operating temperature range	-40 to +75°C (cold startup at -40°C)
Storage temperature range	-40 to +85 °C
Humidity (non-condensing)	5 to 95% RH
Vibration, shock & freefall	IEC68-2-6, -27, -32
Certification compliance	CE/FCC; EN-50121-4
Electrical safety	CSA C22, EN61010-1, CE
EMC	FCC Part 15, CISPR 22 (EN55022) Class A IEC61000-4-2, -3, -4, -5, -6
RoHS and WEEE	RoHS (Pb free) and WEEE compliant
MTBF	> 25 years

Mechanical	
Ingress protection	IP30
Installation option	DIN-Rail mounting, Wall mounting
Dimension	154mm x 109mm x 60mm
Weight	1056g

Quick Installation

Equipment Mounting

Cable Connecting

Equipment Configuration

Quick Installation

Mounting the FSM-510G (DIN-Rail)

Mounting step:

1. Screw the DIN-Rail bracket on with the bracket and screws in the accessory kit.
2. Hook the unit over the DIN rail.
3. Push the bottom of the unit towards the DIN Rail until it snaps into place.

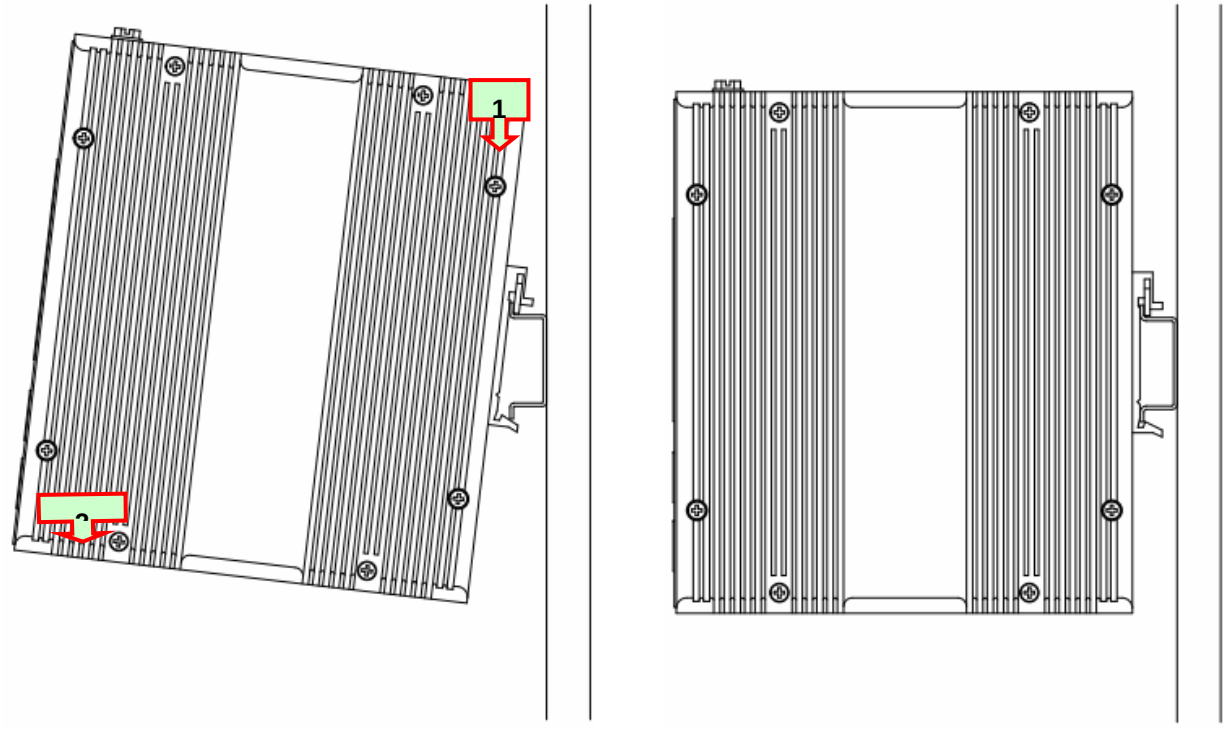


Figure 1 FSM-510G DIN-Rail Mounting

Mounting the FSM-510G (Wall mount)

Mounting step:

1. Screw on the wall-mounting plate on with the plate and screws in the accessory kit.

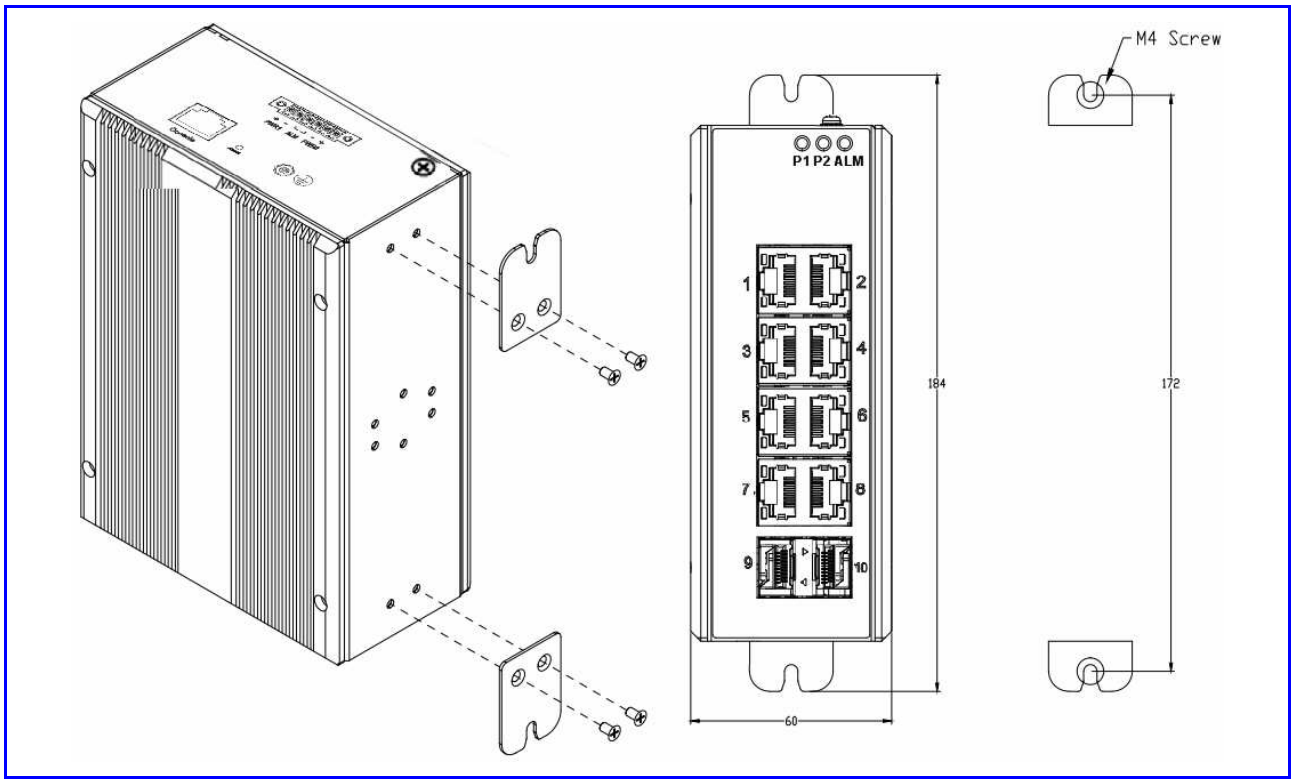
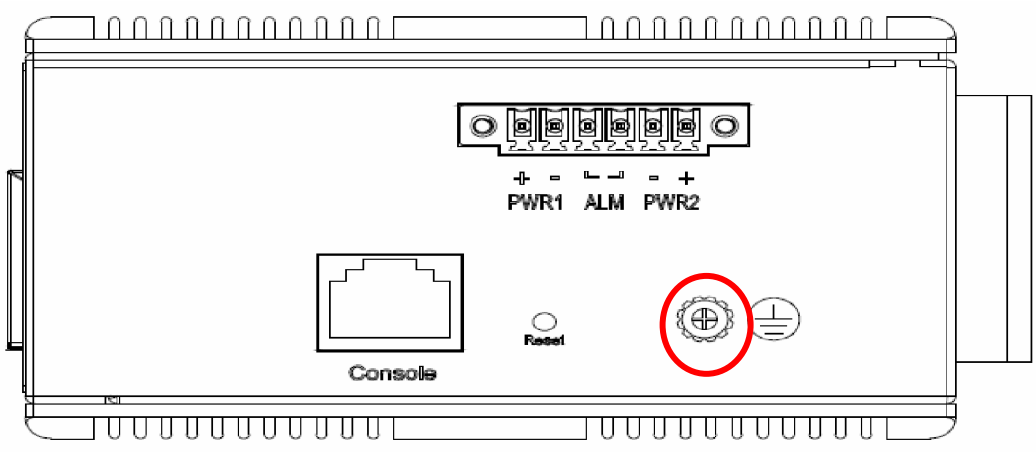


Figure 2 FSM-510G Wall Mounting

Ground Connections

FSM-510G must be properly grounded for optimum system performance.

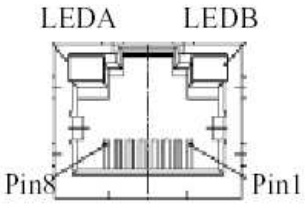


Connecting the Ethernet Interface (RJ45 Ethernet)

FSM-510G provides two types of electrical (RJ45) and optical (mini-GBIC) interfaces. For example, on FSM-510G-2F, Port 1-8 are electrical only (RJ45).

- To connect to a PC, use a straight-through or a cross-over Ethernet cable,
- To connect the FSM-510G copper Port to an Ethernet device, use UTP (Unshielded Twisted Pair) or STP (Shielded Twisted Pair) Ethernet cables.

The pin assignment of RJ-45 connector is shown in the following figure and table.

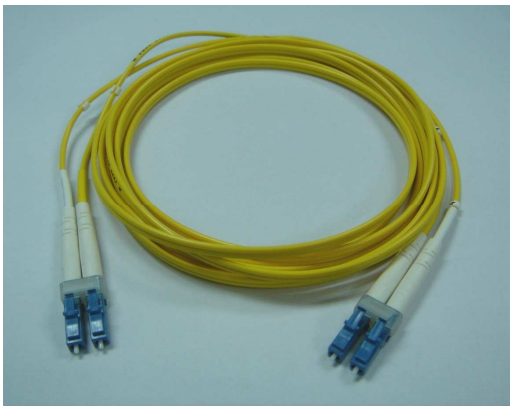


Pin	Assignment
1,2	T/Rx+,T/Rx-
3,6	T/Rx+,T/Rx-
4,5	T/Rx+,T/Rx-
7,8	T/Rx+,T/Rx-

Connecting the Ethernet Interface (Fiber)

Prepare a proper SFP module and install it into the optical port. Then you can connect fiber optics cabling that uses LC connectors or SC connectors (with the use of an optional SC-to-LC adapter) to the fiber optics connector.

Refer to Table 1 for the normal operational LED status.



Fiber optics cable with LC duplex connector

Connect the optical fiber to the SFP socket

DANGER: Never attempt to view optical connectors that might be emitting laser energy.

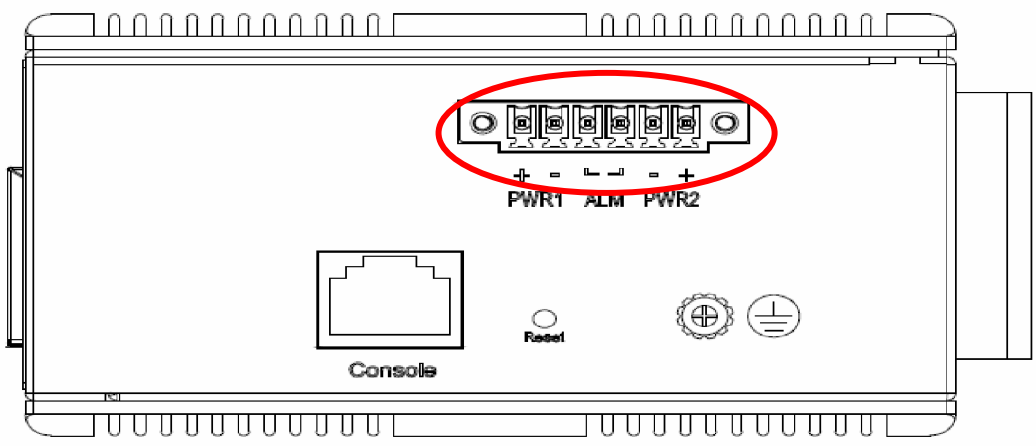
Do not power up the laser product without connecting the laser to the optical fiber and putting the cover in position, as laser outputs will emit infrared laser light at this point.

Power Connection

The DC power interface is a 6-pin terminal block with polarity signs on the top panel.

The FSM-510G can be powered from two power supply (input range 12V – 58V). The DC power connector is a 6-pin terminal block; There is alarm contact on the middle terminal block.

Refer to Table 1 for the normal operational LED status.



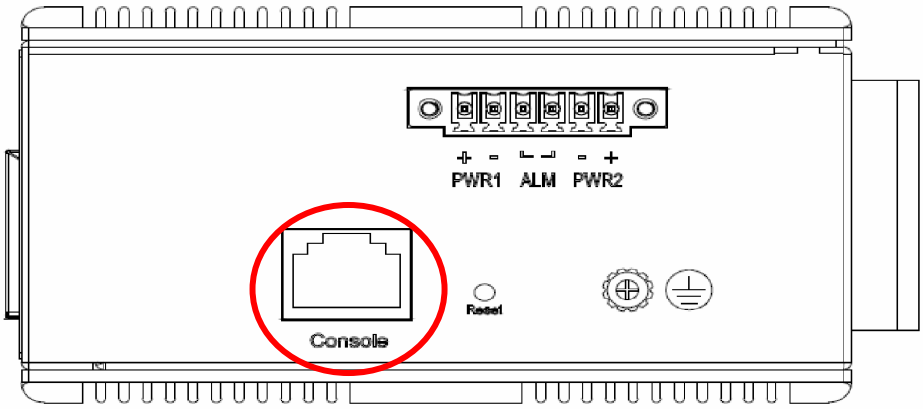
Power Connector (6P Terminal Block)	
Input	DC 12-58V
PWR1 +/-	Power Input 1 +/-
PWR2 +/-	Power Input 2 +/-
ALM	Alarm relay output

Note: 1. The DC power should be connected to a well-fused power supply.

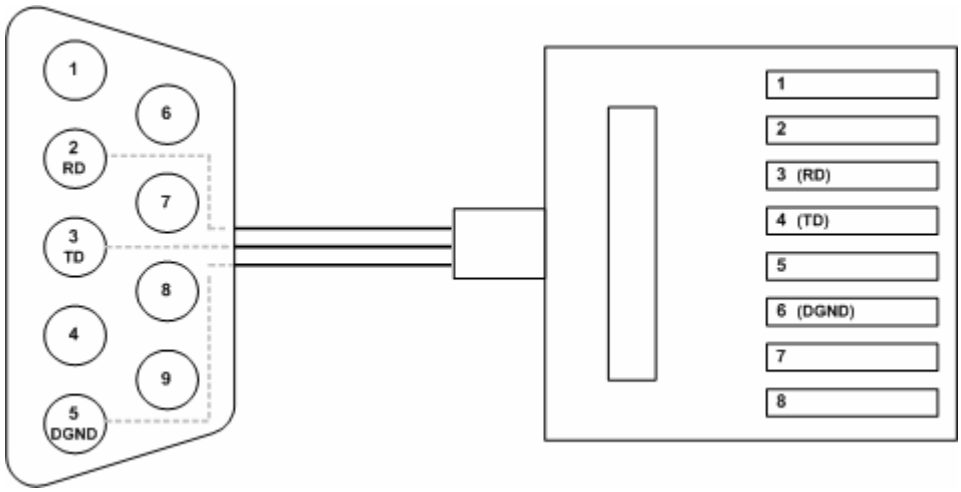
Console Connection

The Console port is for local management by using a terminal emulator or a computer with terminal emulation software.

- DB9 connector connect to computer COM port
- Baud rate: 115200bps
- 8 data bits, 1 stop bit
- None Priority
- None flow control

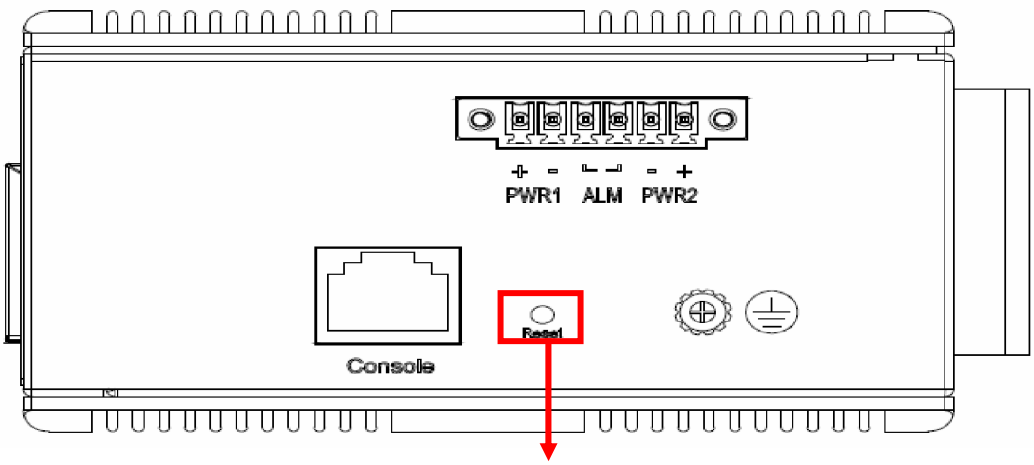


To connect the host PC to the Console port, a RJ45 (male) connector-to-RS232 DB9 (female) connector cable is required. The RJ45 connector of the cable is connected to the Console port of FSM-510G; the DB9 connector of the cable is connected to the PC COM port. The pin assignment of the Console cable is shown below:



SYSTEM RESET

The Reset button is provided to reboot the system without the need to remove power. Under normal circumstances, you will not have to use it. However, or rare occasions, the FSM-510G may not respond; then you may need to push the Reset button.



Reset Button

Web Interface Initialization (Optional)

Web Browser Support

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

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

Firefox with the following default settings is recommended:

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

Google Chrome with the following default settings is recommended:

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

Connect & Login to FSM-510G

1. Connecting to FSM-510G Ethernet port (RJ45 Ethernet port).

2. ***Factory default IP: 192.0.2.1***

3. Login with default account and password.
   Username: admin
   Password: (none)

CLI Initialization & Configuration (Optional)

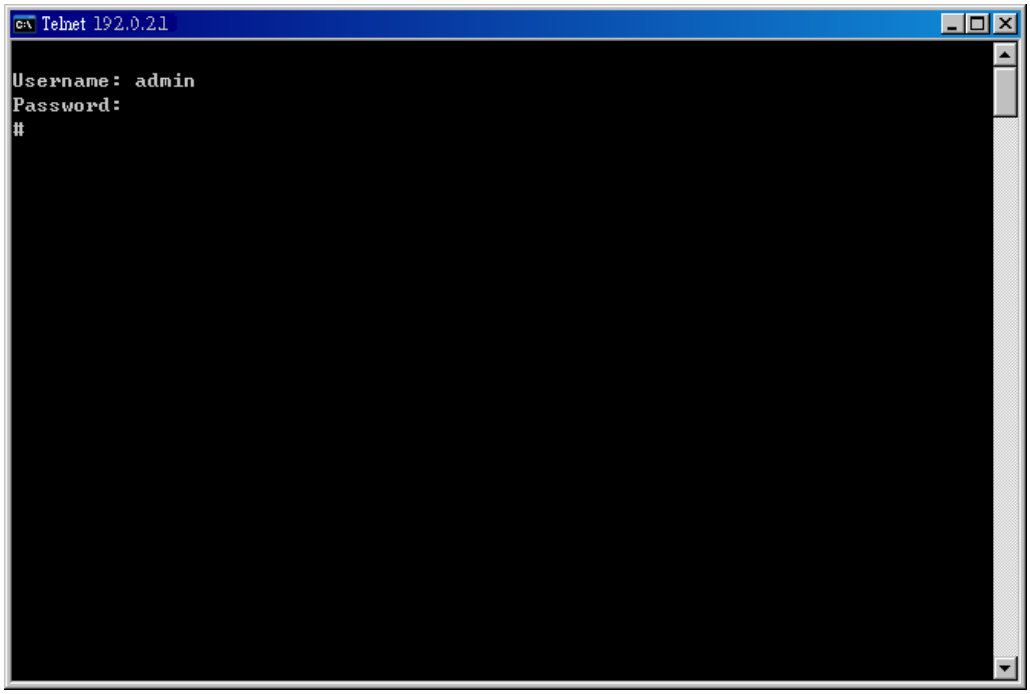
1. Connecting to FSM-510G Ethernet port(RJ45 Ethernet port)

2. Key-in the command under Telnet: ***telnet 192.0.2.1***

3. Login with default account and password.

Username: admin

Password: (none)



4. Change the IP with commands listed below:

<u>CLI Command:</u>

```
enable
configure terminal
interface vlan 1
ip address xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx
exit
```

Monitoring the Ethernet Interface

By RJ45 Ethernet:

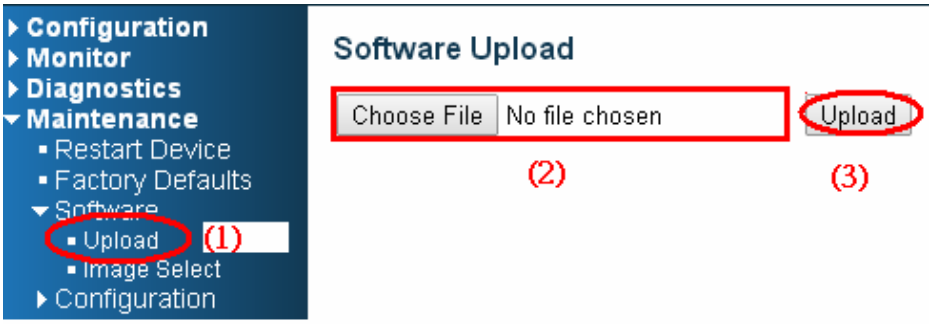
Refer to **Figure 3** for monitoring 8 Gigabit Ethernet with copper connector (RJ45). Also refer to Table 1 for the normal operational LED status.

By SFP:

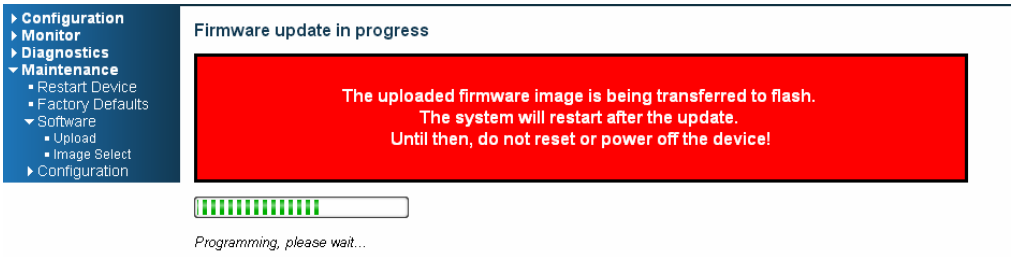
Refer to **Figure 3** for monitoring 4 Gigabit Ethernet with SFP connector. Also refer to Table 1 for the normal operational LED status.

Up/Downgrade Software

1. In Web UI, go to “Maintenance→Software→Upload” page.
2. Select software file, and click “Upload” button.



3. After starting to upload software to device, please don’t cold/warm start device and wait it auto reboot, then upgrade finished.



Reset to Default and Save Configure

Configuration via CLI command

To see what current interface and IP address is:

If manager want to reset the configuration to default but keep management IP setting.

(1) please execute this command: reload defaults keep-ip

(2) check interface VLAN and IP address, confirm only management IP setting kept.

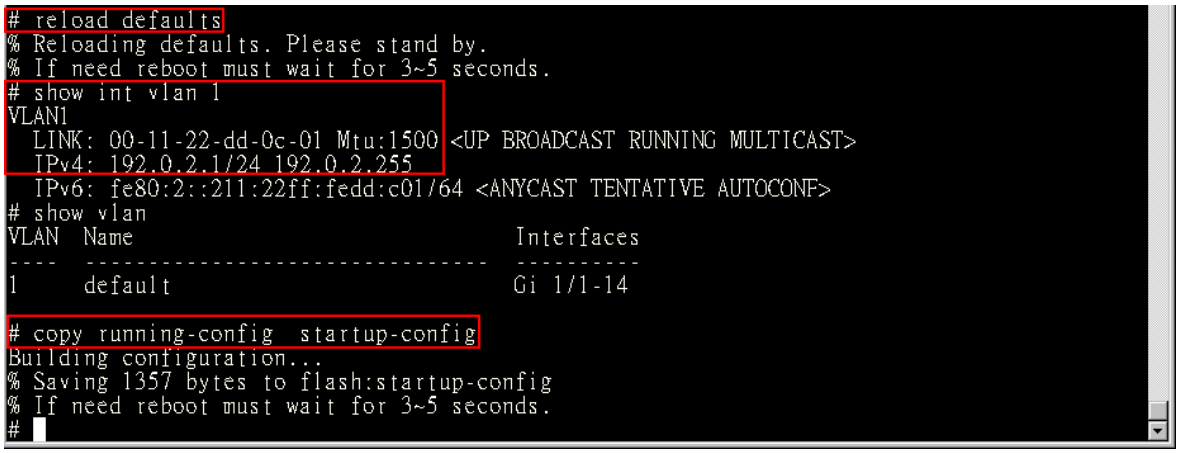
(3) Execute this command: copy running-config startup-config

If manager want to reset the all configuration to default completely

(1) please execute this command: reload defaults

(2) check interface VLAN and IP address, confirm they all change to default setting.

(3) Execute this command: copy running-config startup-config

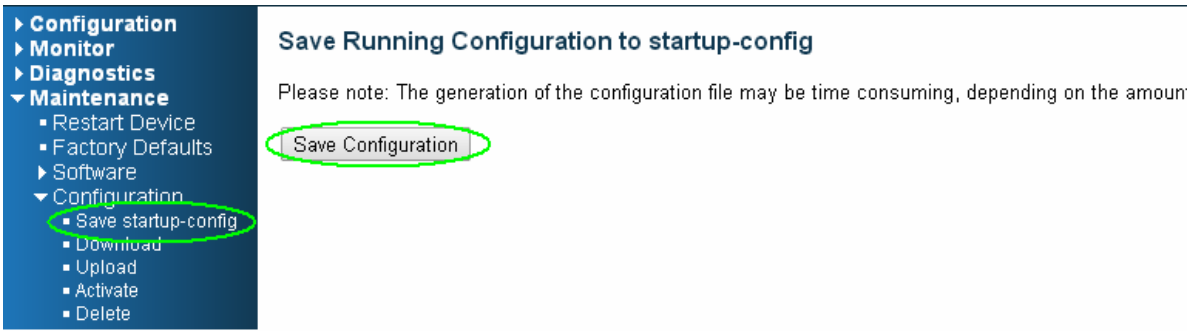


Configuration via WEB UI

If manager want to reset the configuration to default but keep management IP setting

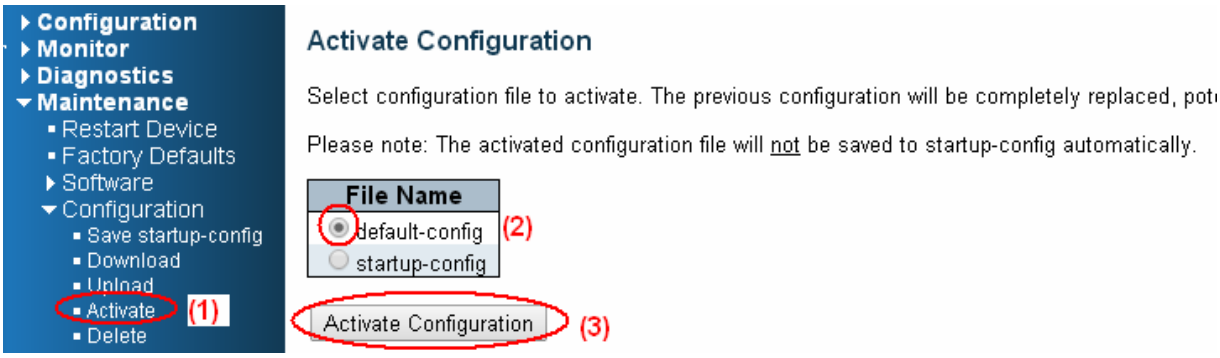
(1)Go to “Maintenance”→”Factory Defaults” pagination to Click “Yes” button.

(2) Go to “Maintenance”→ “Configuration”→”Save startup-config” pagination, then click “Save Configuration” button, then reset successfully.



If manager want to reset the all configuration to default completely

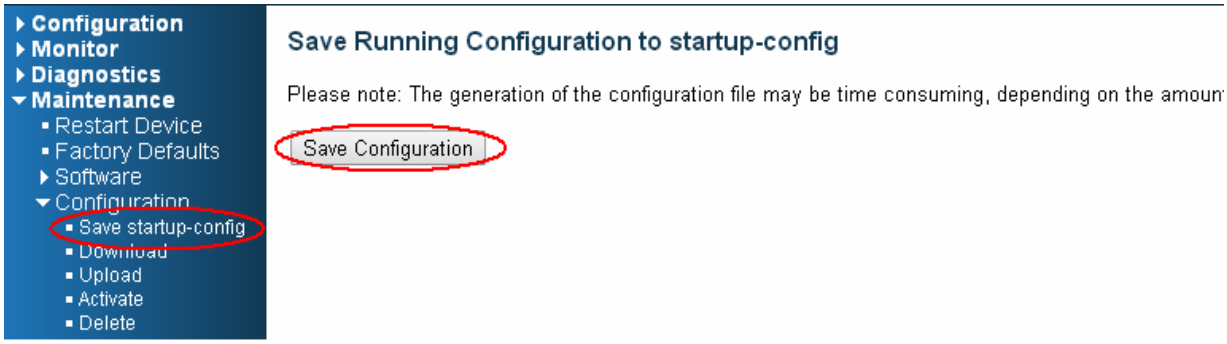
(1) Go to “Maintenance”→ “Configuration”→”Activate” pagination to select “default-config”, then click “Activate Configuration” button



(2) Change PC’s IP address belong to 192.0.2.X networks.

(3) Change WEB's IP be 192.0.2.1(default IP) to login PC's Web UI.

(4) Go to "Maintenance"→ "Configuration"→"Save startup-config" pagination, then click "Save Configuration" button, then reset successfully.



LED STATUS INDICATIONS

Table 1 LED Status Indicators

LED	STATE	Description
P1	On Green	P1 power line has power
	Off	P1 power line disconnect or does not have supply power
P2	On Green	P2 power line has power
	Off	P2 power line disconnect or does not have supply power
Alarm	On Red	Alarm event occurs
	Off	No alarm
Copper ports Link/Act	On Green	Ethernet link up but no traffic is detected
	Flashing Green	Ethernet link up and there is traffic detected
	Off	Ethernet link down
Copper ports Speed	On Yellow	A 100 Mbps or a 1000Mbps connection is detected
	Off	No link or a 10 Mbps connection is detected
SFP port Link/Act	On Green	Ethernet link up
	Off	Ethernet link down
SFP port Speed	On Yellow	SFP port speed 1000Mbps connection is detected.
	Off	No link or a SFP port speed 100Mbps connection is detected

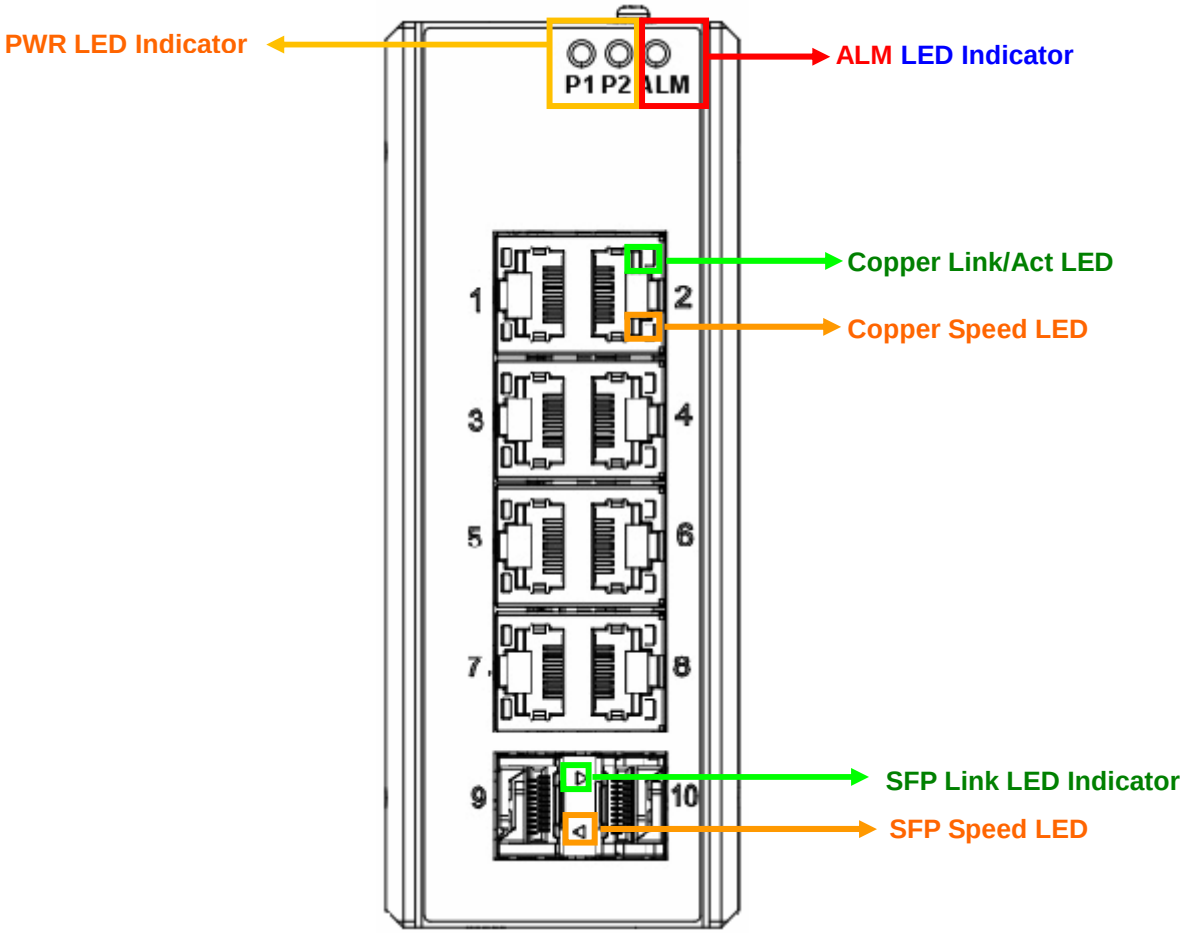


Figure 3 LED Indicators

Application Guide

VLAN Application Guide
Security Application Guide
Ring Protection Application Guide
QoS Application Guide
Link Fail Alarm Application Guide
802.1x Authentication Application Guide

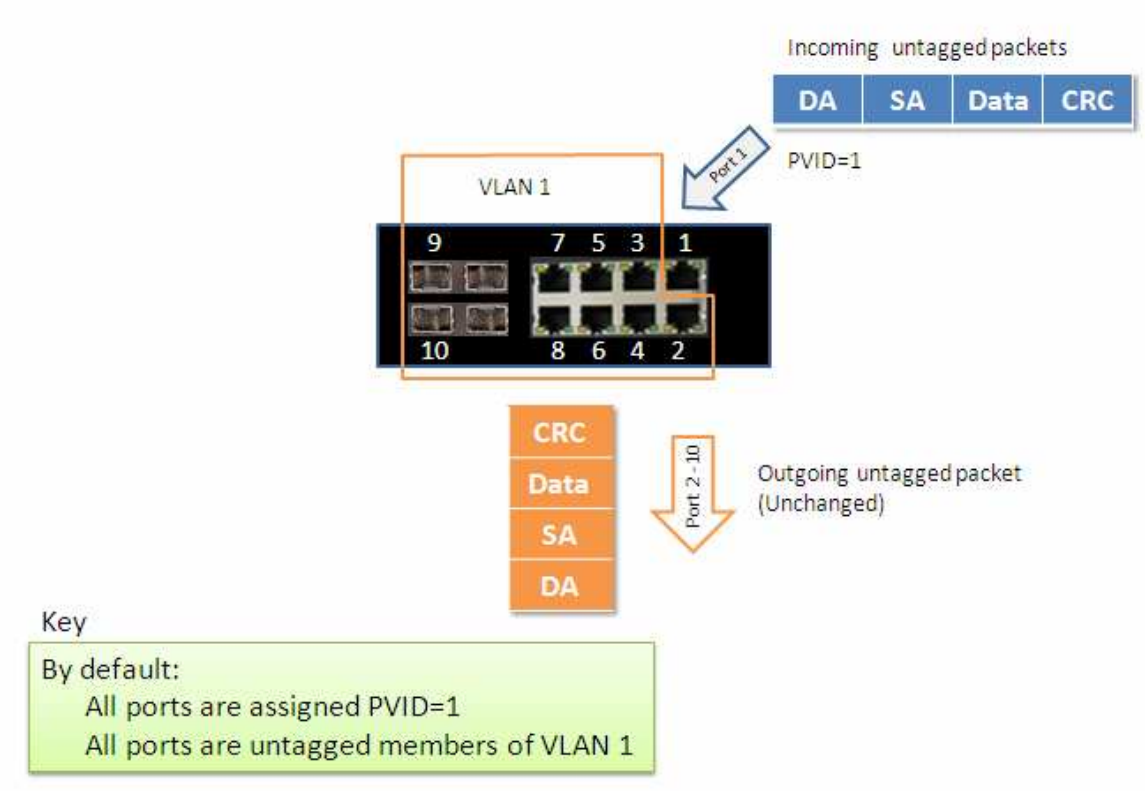
VLAN Application Guide

This part describes how to configure Virtual LANs (VLANs) in FSM-510G. The FSM-510G supports up to 2048 VLANs. Ports are grouped into broadcast domains by assigning them to the same VLAN. Frames received in on VLAN can only be forwarded within that VLAN, and multicast frames and unknown unicast frames are flooded only to ports in the same VLAN.

Example 1: Default VLAN Settings

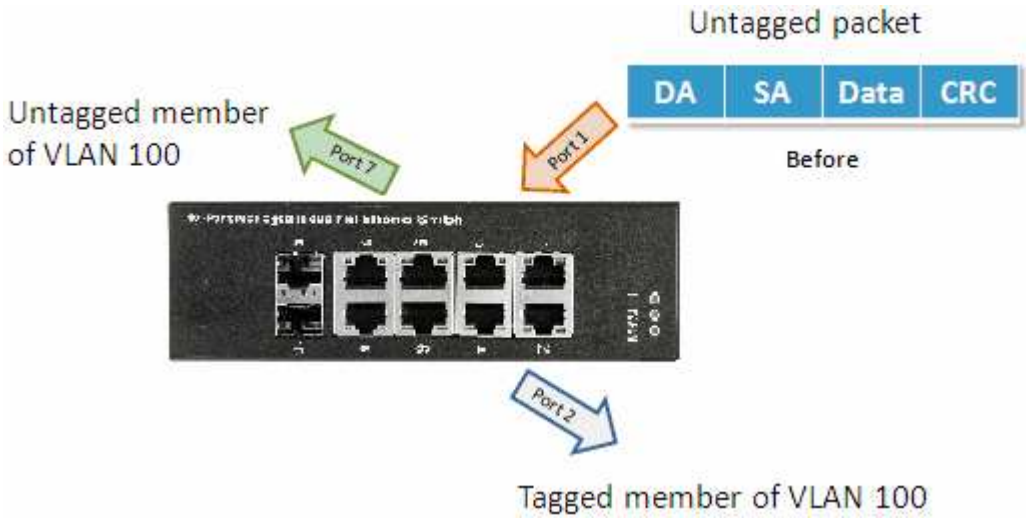
Each port in the FSM-510G has a configurable default VLAN number, known as its PVID. This places all ports on the same VLAN initially, although each port PVID is configurable to any VLAN number between 1 and 4094.

The default configuration settings for FSM-510G have all ports set as untagged members of VLAN 1 with all ports configured as PVID=1. In default configuration example shown in the following figure, all incoming packets are assigned to VLAN 1 by the default port VLAN identifier (PVID=1).



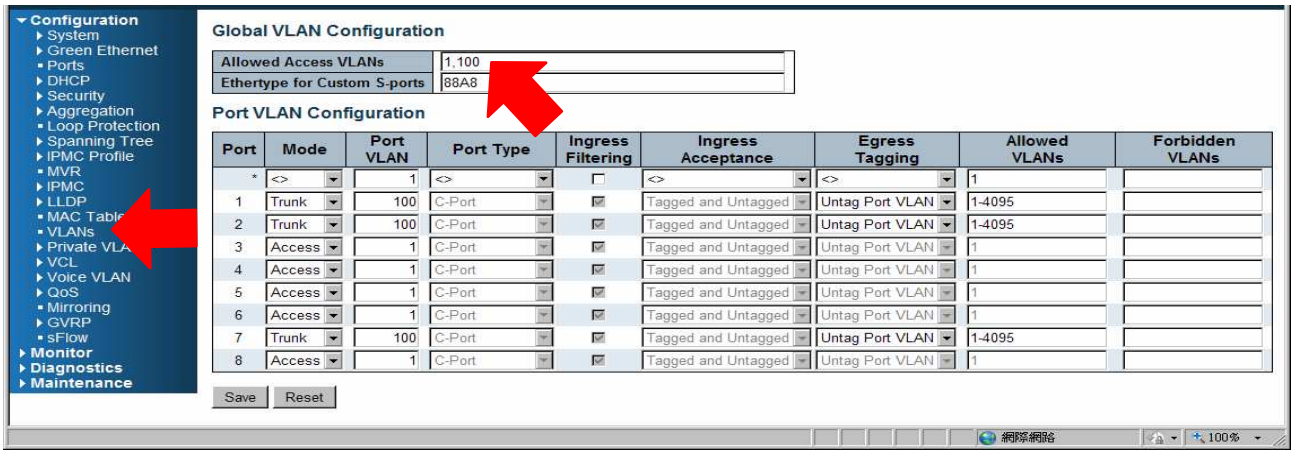
Example 2: Port-based VLANs

When the FSM-510G receives an untagged VLAN packet, it will add a VLAN tag to the frame according to the PVID setting on a port. As shown in the following figure, the untagged packet is marked (tagged) as it leaves the FSM-510G through Port 2, which is configured as a tagged member of VLAN100. The untagged packet remains unchanged as it leaves the FSM-510G through Port 7, which is configured as an untagged member of VLAN100.



Configuration:

Step1. Go to Configuration -> VLANs -> Port VLAN configuration and configure PVID 100 on Port 1, Port 2 and Port 7.



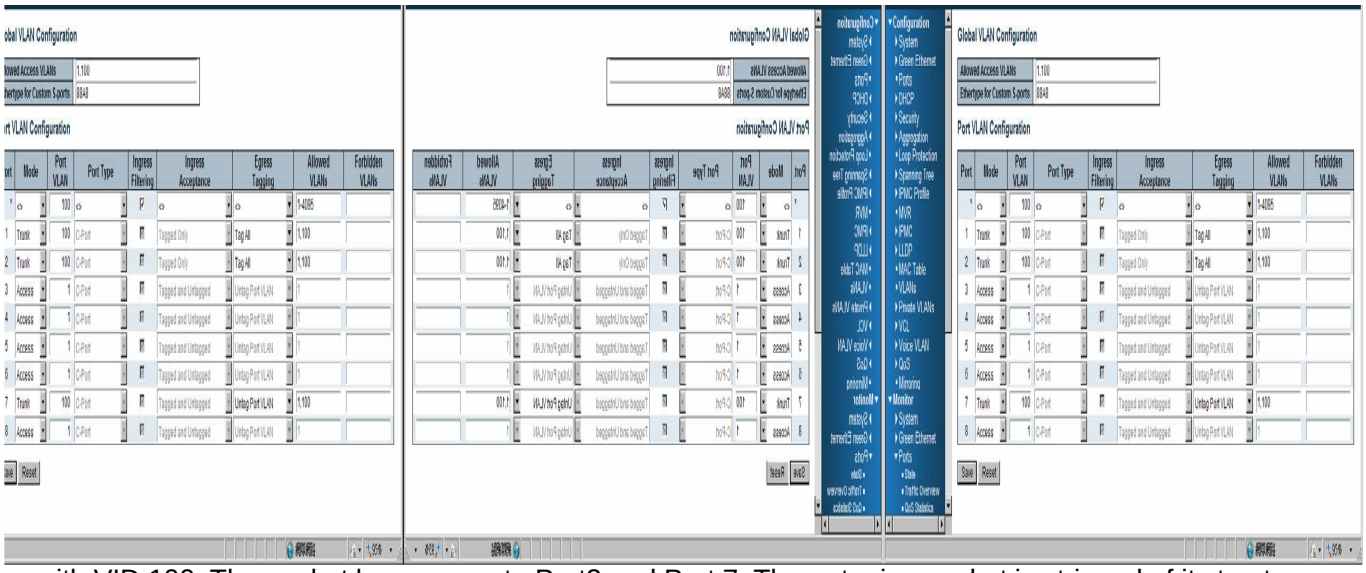
Step2. Select Configuration -> VLAN -> Static VLAN. Create a VLAN with VLAN ID 100. Enter a VLAN name in the **Name** field.

Step3. Assign VLAN tag setting to or remove it from a port by toggling the check box under an individual port number. The tag settings determine if packets that are transmitted from the port tagged or untagged with the VLAN ID. The possible tag settings are:

Tag All	Specifies that the egress packet is tagged for the port.
Untag port vlan	Specifies that the egress packet is untagged for the port.
Untag All	Specifies that all frames, whether classified to the Port VLAN or not, are transmitted without a tag.

Here we set tagged VLAN100 on Port 1 and Port 2, untagged VLAN100 on Port7.

Step4. Transmit untagged unicast packets from Port 1 to Port 2 and Port 7. The FSM-510G should tag it



with VID 100. The packet has access to Port2 and Port 7. The outgoing packet is stripped of its tag to leave Port 7 as an untagged packet. For Port 2, the outgoing packet leaves as a tagged packet with VID 100.

Step5. Transmit untagged unicast packets from Port 2 to Port 1 and Port 7. The FSM-510G should tag it with VID 100. The packet has access to Port1 and Port 7. The outgoing packet is stripped of its tag to leave Port 7 as an untagged packet. For Port 1, the outgoing packet leaves as a tagged packet with VID 100.

Step6. Transmit untagged unicast packets from Port 7 to Port 1 and Port 2. The FSM-510G should tag it with VID 100. The packet has access to Port1 and Port 2. For Port 1 and Port 2, the outgoing packet leaves as a tagged packet with VID 100.

Step7. Repeat step 4 using broadcast and multicast packets.

CLI Command:

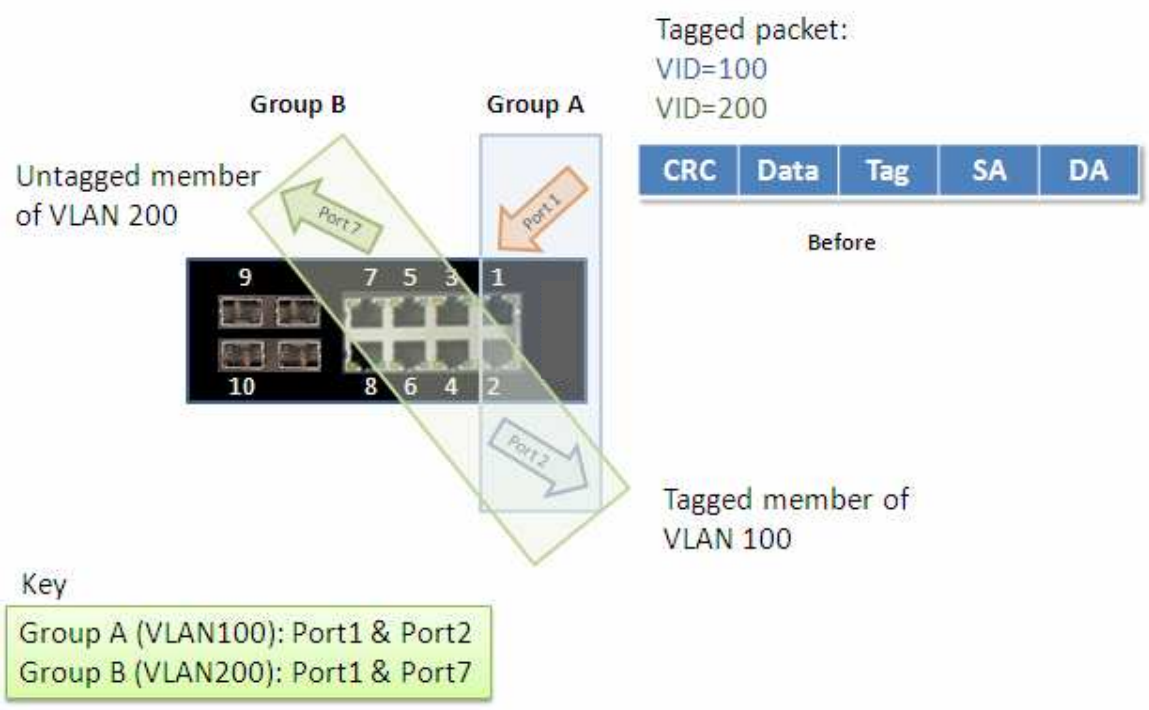
```
vlan 1
vlan 100

interface GigabitEthernet 1/1
switchport access vlan 100
switchport trunk native vlan 100
switchport trunk allowed vlan 1,100
switchport trunk vlan tag native
switchport mode trunk
exit
interface GigabitEthernet 1/2
switchport access vlan 100
switchport trunk native vlan 100
switchport trunk allowed vlan 1,100
switchport trunk vlan tag native
switchport mode trunk
exit
interface GigabitEthernet 1/7
switchport access vlan 100
switchport trunk native vlan 100
switchport trunk allowed vlan 1,100
switchport mode trunk
exit
```

Example 3: IEEE 802.1Q Tagging

FSM-510G is able to construct layer-2 broadcast domain by identifying VLAN ID specified by IEEE 802.1Q. It forwards a frame between bridge ports assigned to the same VLAN ID and can set multiple VLANs on each bridge port.

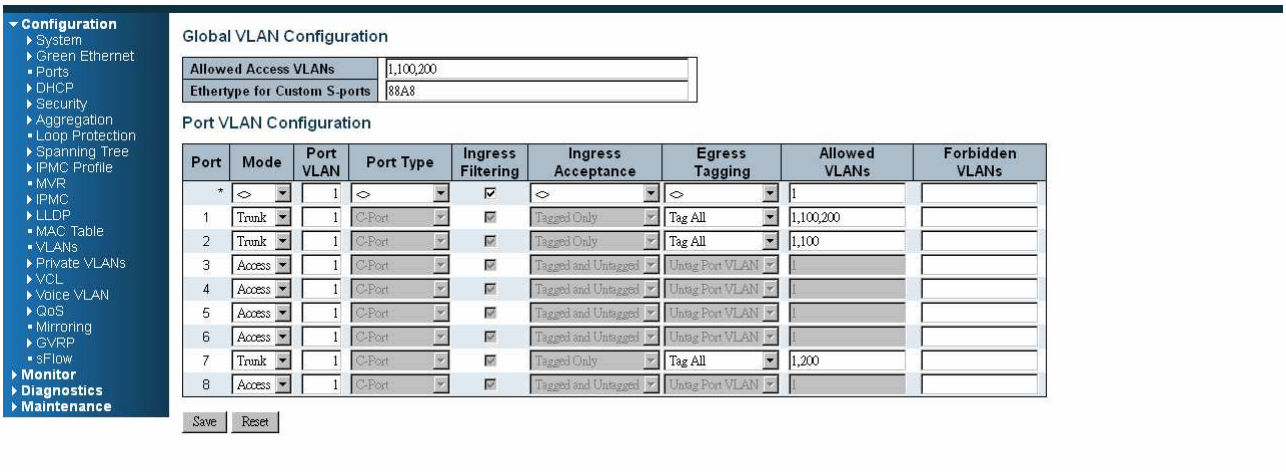
In the following figure, the tagged incoming packets are assigned directly to VLAN 100 and VLAN 200 because of the tag assignment in the packet. Port 2 is configured as a tagged member of VLAN 100, and Port 7 is configured as an untagged member of VLAN 200. Hosts in the same VLAN communicate with each other as if they in a LAN. However, hosts in different VLANs cannot communicate with each other directly.



In this case:
1. The hosts from Group A can communicate with each other.
2. The hosts from Group B can communicate with each other.
3. The hosts of Group A and Group B can’t communicate with each other.
4. Both the Group A and Group B can go to Internet through IVS514F.

Configuration:

Step1. Go to C onfiguration -> VLANs -> Port VLAN configuration page specify the VLAN membership as follows:



Step2. Transmit unicast packets with VLAN tag 100 from Port 1 to Port 2 and Port 7. The FSM-510G should tag it with VID 100. The packet only has access to Port2. For Port 2, the outgoing packet leaves as a tagged packet with VID 100.

Step3. Transmit unicast packets with VLAN tag 200 from Port 1 to Port 2 and Port 7. The FSM-510G should tag it with VID 200. The packet only has access to Port7. The outgoing packet on Port 7 is stripped of its tag as an untagged packet.

Step4. Transmit unicast packets with VLAN tag 100 from Port 2 to Port 1 and Port 7. The FSM-510G should tag it with VID 100. The packet only has access to Port1. For Port 1, the outgoing packet leaves as a tagged packet with VID 100.

Step5. Transmit unicast packets with VLAN tag 200 from Port 7 to Port 1 and Port 2. The FSM-510G should tag it with VID 200. The packet only has access to Port1. The outgoing packet on Port 1 will leave as a tagged packet with VID 200.

Step6. Repeat the above steps using broadcast and multicast packets.

CLI Command:

```
vlan 100
vlan 200

interface GigabitEthernet 1/1
switchport access vlan 100
switchport trunk allowed vlan 1,100,200
switchport trunk vlan tag native
switchport mode trunk
exit
interface GigabitEthernet 1/1
switchport access vlan 100
switchport trunk allowed vlan 1,100
switchport trunk vlan tag native
switchport mode trunk
exit

interface GigabitEthernet 1/7
switchport access vlan 100
switchport trunk allowed vlan 1,200
switchport trunk vlan tag native
switchport mode trunk
exit
```

Security Application Guide

ACL function supports access control security for MAC address, IP address, Layer4 Port, and Type of Service. Each has five actions: Deny, Permit, Queue Mapping, CoS Marking, and Copy Frame. User can set default ACL rule to Permit or Deny. To get more clearly for these ACL function, see following table.

Default ACL Rule	Actions				
	Deny	Permit	Queue Mapping	CoS Marking	Copy Frame
Permit	(a)	(b)	(c)	(d)	(e)
Deny	(f)	(g)	(h)	(i)	(j)

Brief descriptions of the above table:
(a): Permit all frames, but deny frames set in ACL entry.
(b): Permit all frames.
(c): Permit all frames, and to do queue mapping of the transmitting frames.
(d): Permit all frames, and to change CoS value of the transmitting frames.
(e): Permit all frames, and to copy frame which set in ACL entry to a defined GE port.
(f): Deny all frames.
(g): Deny all frames, but permit frames set in ACL entry.
(h): Deny all frames.
(i): Deny all frames.
(j): Deny all frames, but to copy frame which set in ACL entry to a defined GE port.

Case 1: ACL for MAC address

For MAC address ACL, it can filter on source MAC address, destination MAC address, or both. When it filters on both MAC address, packets coincident with both rules will take effect. In other words, it does not do filter if it only coincident with one rule.

If user want to filter only one directional MAC address, the other MAC address just set to all zero. It means don't care portion. Besides MAC address, it also supports VLAN and Ether type for filter additionally. Certain VLAN or Ether type under these MAC address will take effect. If user doesn't care VLAN or Ether type, he can just set to zero values. Following are examples about the above table:

- **Case 1:** (a)

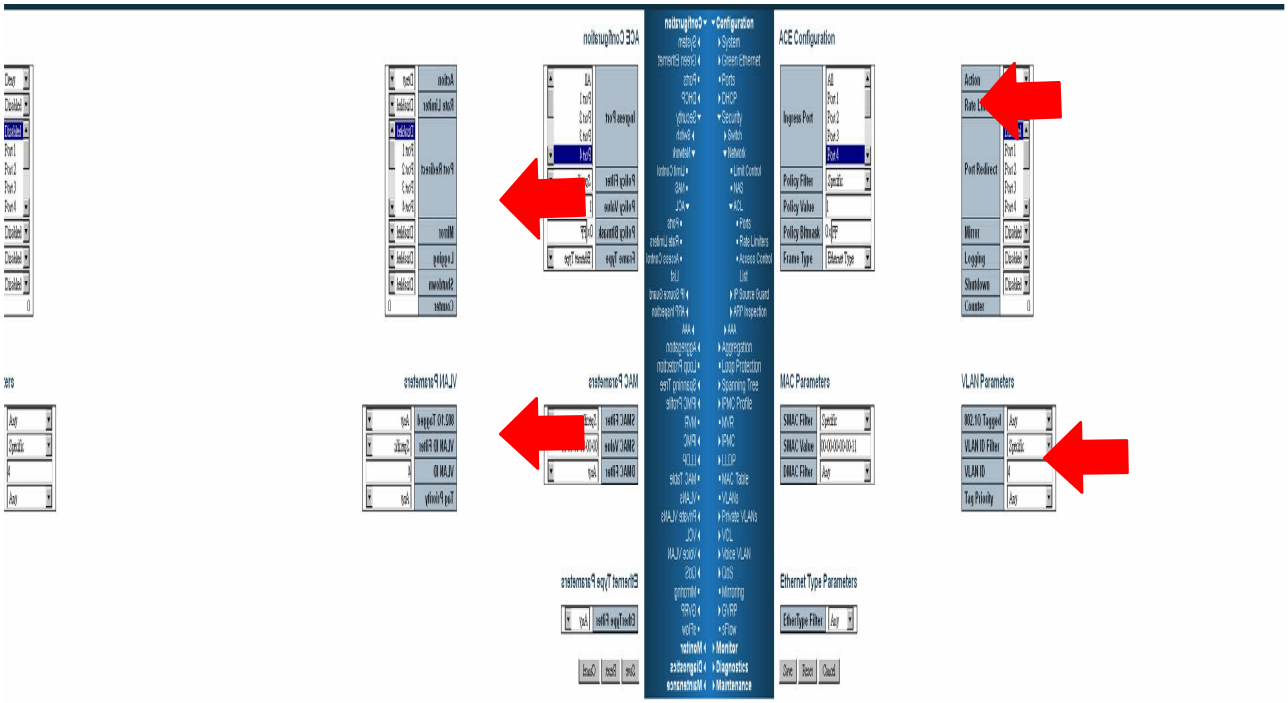
User can set default ACL Rule of GE port as "Permit", then to bind a suitable profile with "deny" action for ACL. It means GE port can pass through all packets but not ACL entry of the profile binding.

◎ One directional MAC address with one VLAN deny filtering.

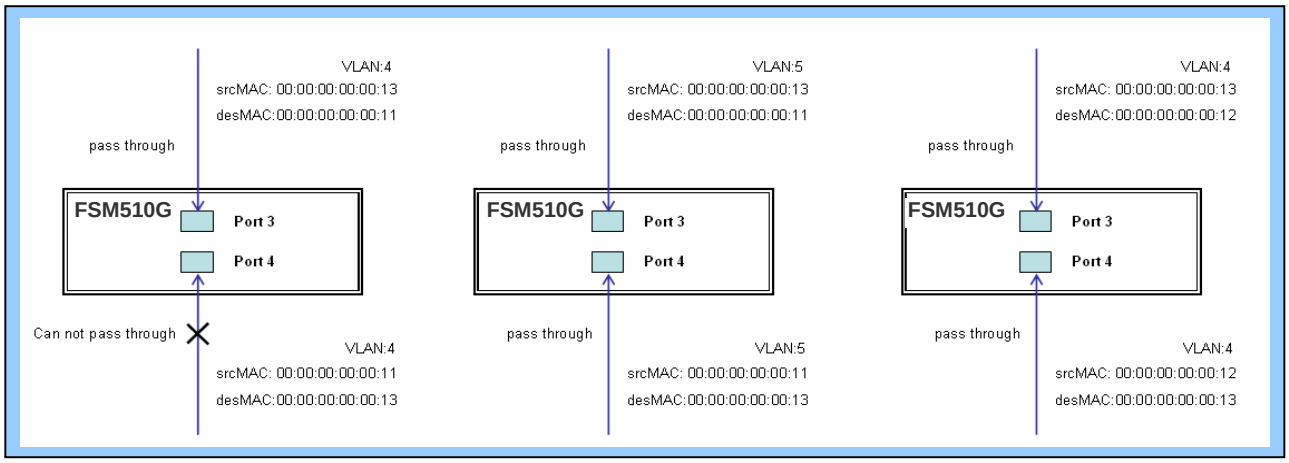
Step 1: Create a new ACL Profile. (Profile Name: DenySomeMac)

Step 2: Create a new ACL Entry rule under this ACL profile. (Deny MAC: 11 and VLAN: 4)

Step 3: Bind this ACL profile to a GE port. (PORT-4)



Step 4: Send frames between PORT-3 and PORT-4, and see test result.



CLI Command:

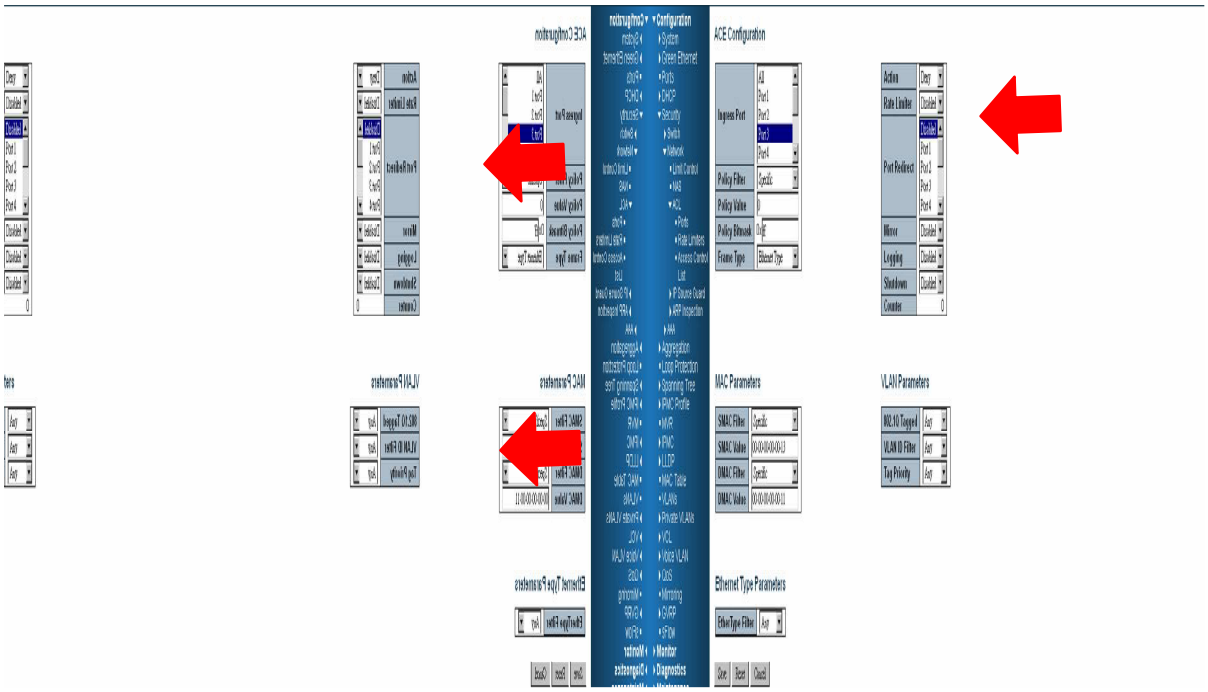
```
access-list ace 1 ingress interface GigabitEthernet 1/4 policy 1 vid 4
frametype etype smac 00-00-00-00-00-11 action deny
exit
interface GigabitEthernet 1/3
  switchport trunk allowed vlan 4,5
  switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
  switchport trunk allowed vlan 4,5
  switchport trunk vlan tag nativevlan 4
exit
```

◎ Two directional MAC address with all VLAN deny filtering.

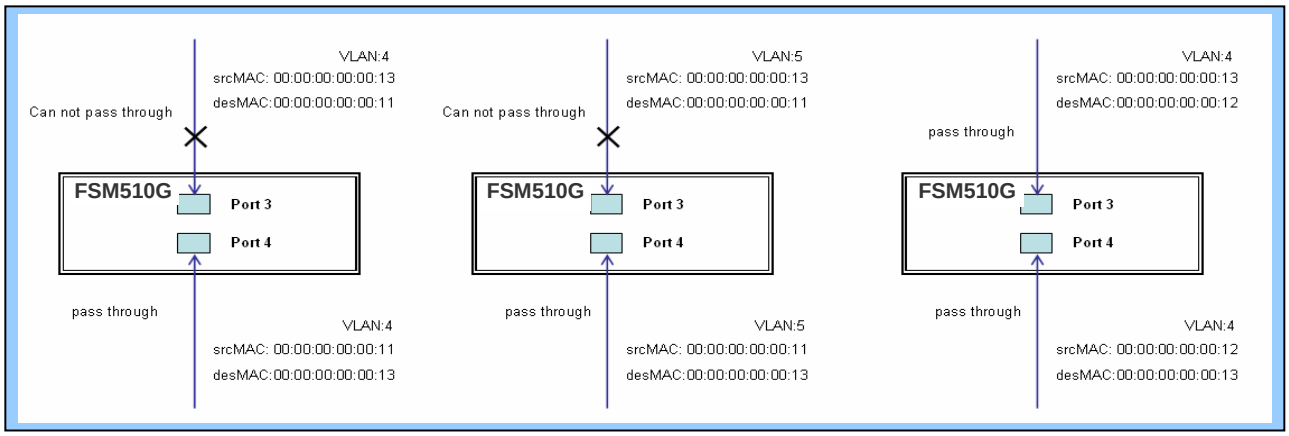
Step 1: Create a new ACL Profile. (Profile Name: DenySomeMac)

Step 2: Create a new ACL Entry rule under this ACL profile. (Deny SrcMAC: 13 and DesMAC: 11)

Step 3: Bind this ACL profile to a GE port. (PORT-3)



Step 4: Send frames between PORT-3 and PORT-4, and see test result.



CLI Command:

```
access-list ace 2 ingress interface GigabitEthernet 1/3 policy 0 frametype etype smac
00-00-00-00-00-13 dmac 00-00-00-00-00-11 action deny
exit
interface GigabitEthernet 1/3
  switchport trunk allowed vlan 4,5
  switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
  switchport trunk allowed vlan 4,5
  switchport trunk vlan tag nativevlan 4
exit
```

- **Case 1: (b)**

This case acts as no ACL function. It means all frames will pass through.

- **Case 1: (c)**

User can set default ACL Rule of GE port as “Permit”, then to bind a suitable profile with “Queue Mapping” action for some ACL function. It means GE port can do queue mapping 0~7 of the frame received from this port.

- **Case 1: (d)**

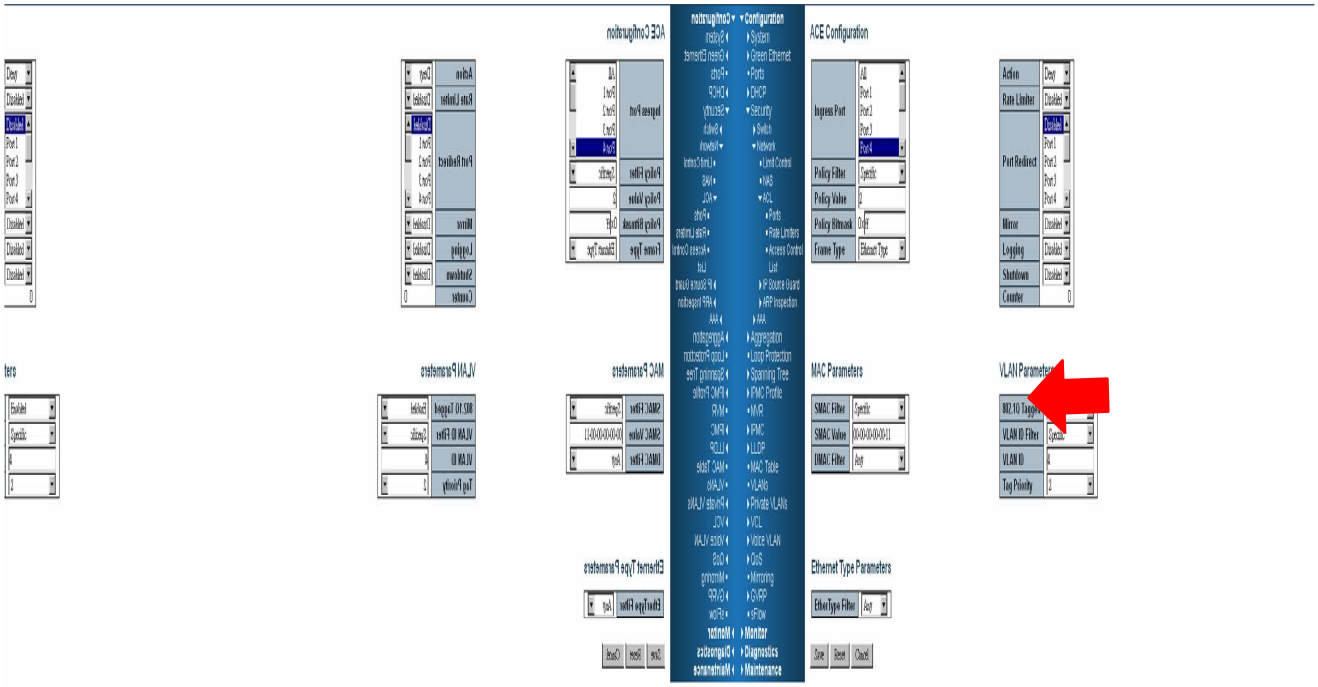
User can set default ACL Rule of GE port as “Permit”, then to bind a suitable profile with “CoS Marking” action for some ACL function. It means GE port can remark CoS of the VLAN frame received from this port.

◎ One directional MAC address with CoS Marking action. (one VLAN, and don’t care Ether Type)

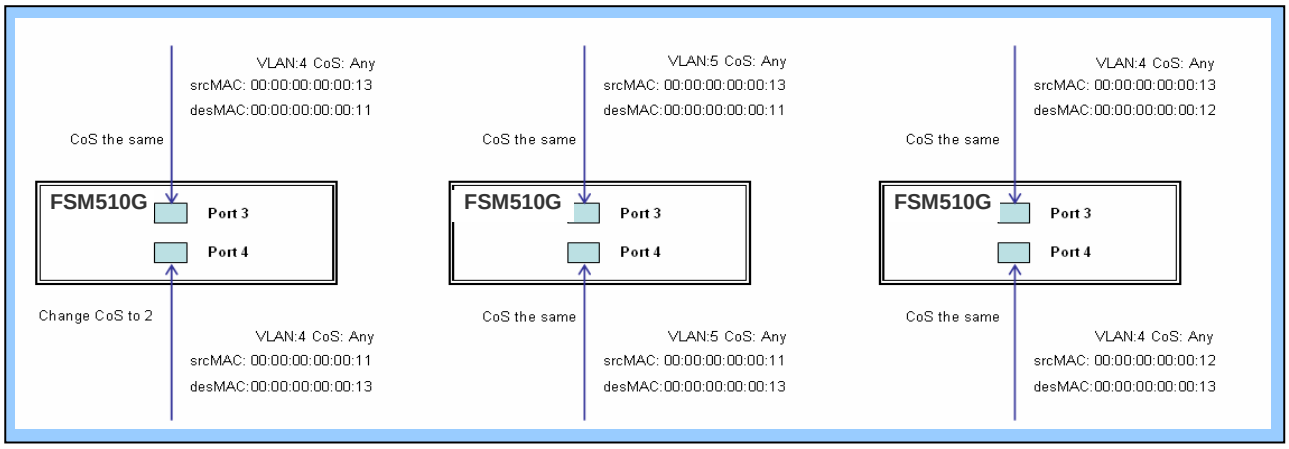
Step 1: Create a new ACL Profile. (Profile Name: CoSMarkingTest)

Step 2: Create a new ACL Entry rule under this ACL profile.
(Filter SrcMAC: 11 and VLAN ID: 4 frame to CoS: 2)

Step 3: Bind this ACL profile to a GE port. (PORT-4)



Step 4: Send frames between PORT-3 and PORT-4, and see test result.



CLI Command:

```
access-list ace 1 next 2 ingress interface GigabitEthernet 1/4 policy 1 vid 4 frametype etype
smac 00-00-00-00-00-11 action deny
exit
interface GigabitEthernet 1/3
  switchport trunk allowed vlan 4,5
  switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
  switchport trunk allowed vlan 4,5
  switchport trunk vlan tag native
exit
```

- **Case 1: (e)**

User can set default ACL Rule of GE port as “Permit”, then to bind a suitable profile with “Copy Frame” action for mirror analyzer used. It means the system will copy frames from binding GE Port to analyzer port.

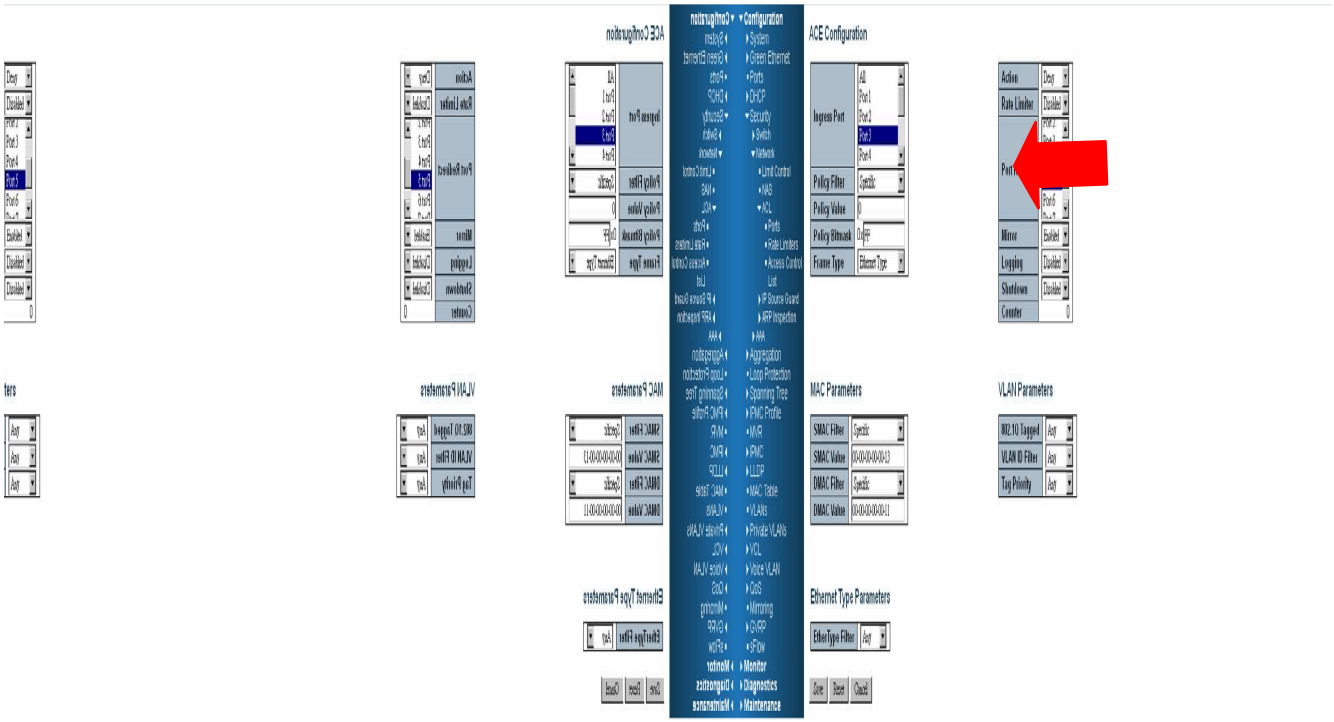
◎ Two directional MAC address with Copy Frame action.
(Don’t care VLAN ID, Ether Type)

Step 1: Create a new ACL Profile. (Profile Name: CopyFrameTest)

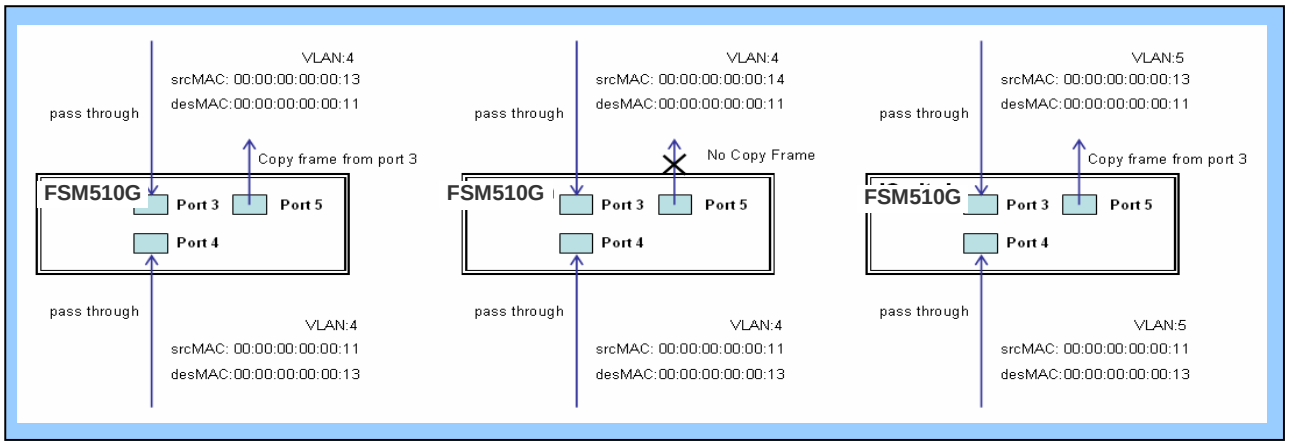
Step 2: Create a new ACL Entry rule under this ACL profile. (SrcMAC: 13 and DesMAC: 11)

Step 3: Set analyzer port to enable and mirror analyzer port.

Step 4: Bind this ACL profile to a GE port. (PORT-3)



Step 5: Send frames between PORT-3 and PORT-4, and see test result.



CLI Command:

```
access-list ace 2 next 3 ingress interface GigabitEthernet 1/3 policy 0 frametype etype smac
00-00-00-00-00-13 dmac 00-00-00-00-00-11 action deny mirror redirect interface
GigabitEthernet 1/5
exit
interface GigabitEthernet 1/3
  switchport trunk allowed vlan 4,5
  switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
  switchport trunk allowed vlan 4,5
  switchport trunk vlan tag native
exit
```

- ***Case 1: (f)***

This case means all frames will not pass through.

- ***Case 1: (g)***

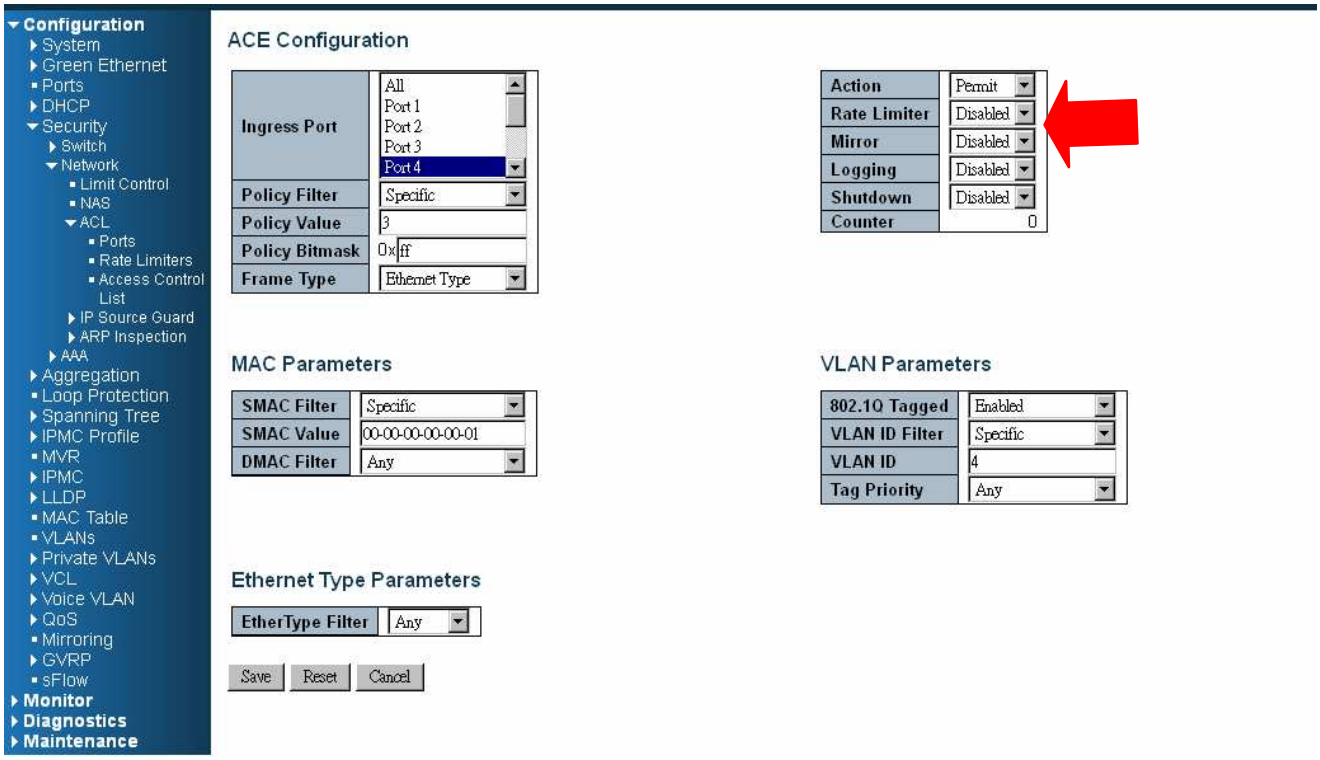
User can set default ACL Rule of GE port as “Deny”, then to bind a suitable profile with “Permit” action for ACL. It means GE port can not pass through all packets but ACL entry of the profile binding.

◎ One directional MAC address with one VLAN permit filtering.

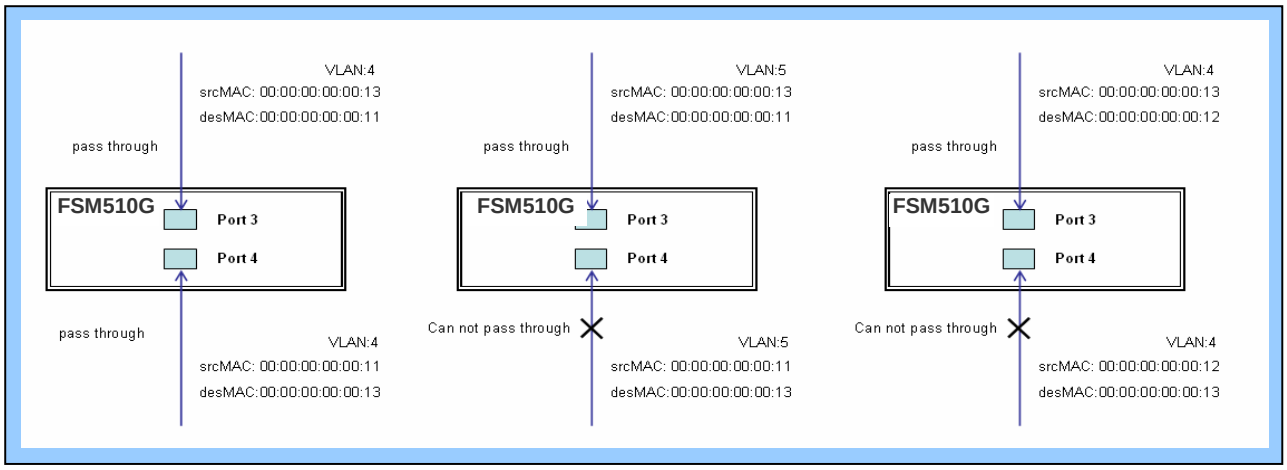
Step 1: Create a new ACL Profile. (Profile Name: AllowSomeMac)

Step 2: Create a new ACL Entry rule under this ACL profile. (Allow MAC: 11 and VLAN: 4)

Step 3: Bind this ACL profile to a GE port. (PORT-4)



Step 4: Send frames between PORT-3 and PORT-4, and see test result.



CLI Command:

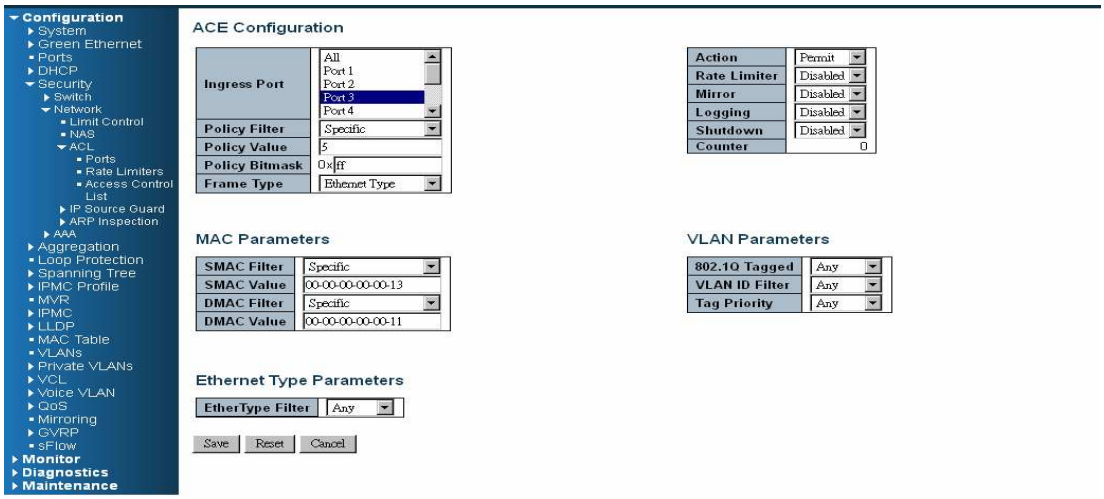
```
access-list ace 4 ingress interface GigabitEthernet 1/4 policy 3 tag tagged vid 4 frametype etype
smac 00-00-00-00-00-11
exit
  interface GigabitEthernet 1/3
  switchport trunk allowed vlan 4,5
  switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
  switchport trunk allowed vlan 4,5
  switchport trunk vlan tag native
exit
```

◎ Two directional MAC address with all VLAN permit filtering.

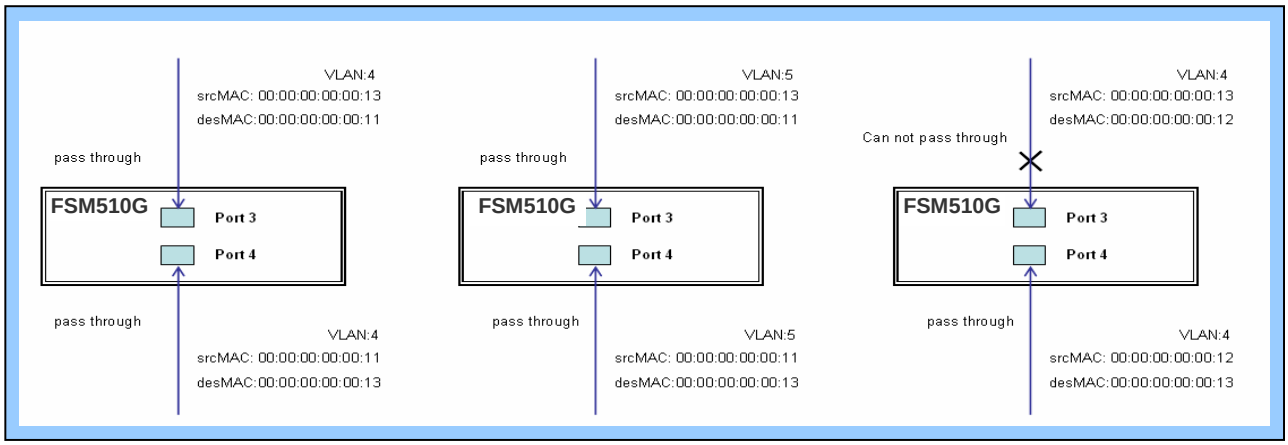
Step 1: Create a new ACL Profile. (Profile Name: AllowSomeMac)

Step 2: Create a new ACL Entry rule under this ACL profile. (Allow SrcMAC: 13 and DesMAC: 11)

Step 3: Bind this ACL profile to a GE port. (PORT-3)



Step 4: Send frames between PORT-3 and PORT-4, see test result.



CLI Command:

```
access-list ace 5 ingress interface GigabitEthernet 1/3 policy 5 frametype etype smac
00-00-00-00-00-13 dmac 00-00-00-00-00-11
exit
interface GigabitEthernet 1/3
  switchport trunk allowed vlan 4,5
  switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
  switchport trunk allowed vlan 4,5
  switchport trunk vlan tag native
exit
```

- **Case 1: (h)**

Because the default ACL Rule of GE port is “Deny”, Queue Mapping action has no sense. We do not do this case.

- **Case 1: (i)**

Because the default ACL Rule of GE port is “Deny”, CoS Marking action has no sense. We do not do this case.

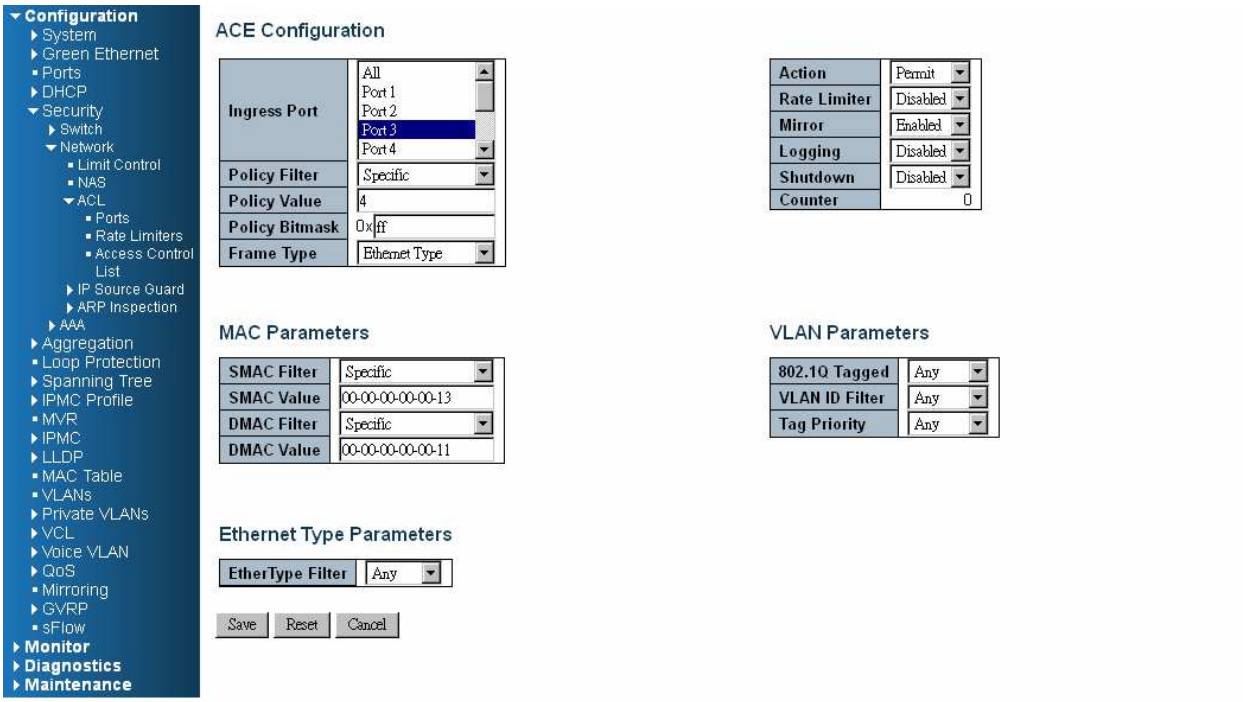
- **Case 1: (j)**

User can set default ACL Rule of GE port as “Deny”, then to bind a suitable profile with “Copy Frame” action for mirror analyzer used. It means the system will copy frames from binding GE Port to analyzer port. There is no frame received from the denied GE port but the mirror analyzer port.

◎ One directional MAC address with Copy Frame action. (Don’t case VLAN, Ether Type)

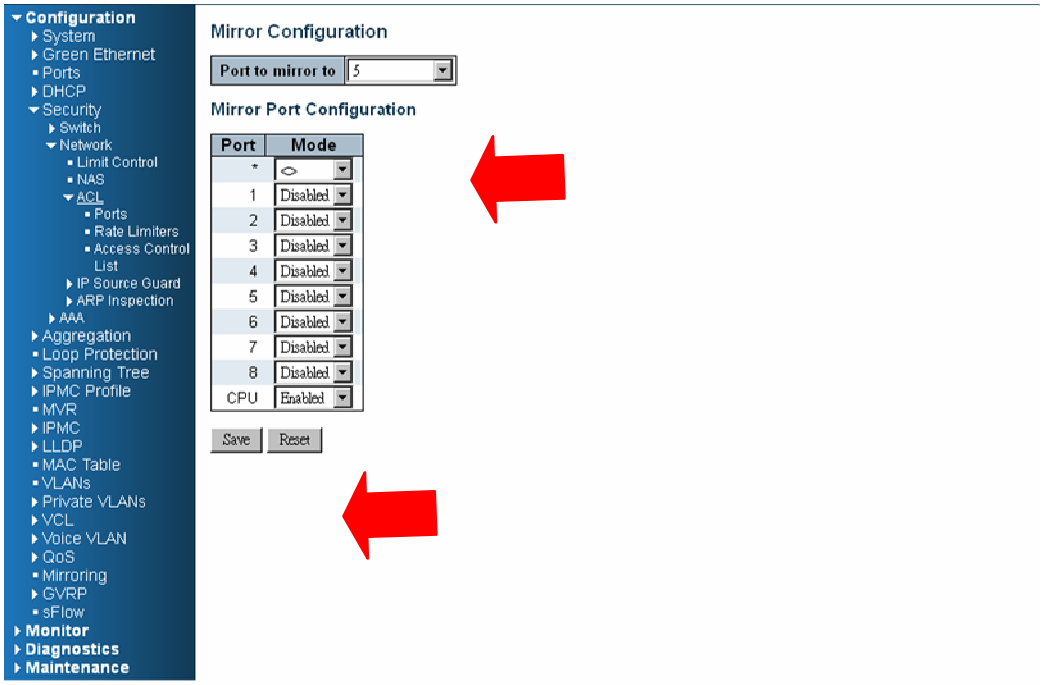
Step 1: Create a new ACL Profile. (Profile Name: CopyFrameTest)

Step 2: Create a new ACL Entry rule under this ACL profile. (SrcMAC: 13 and DesMAC: 11)

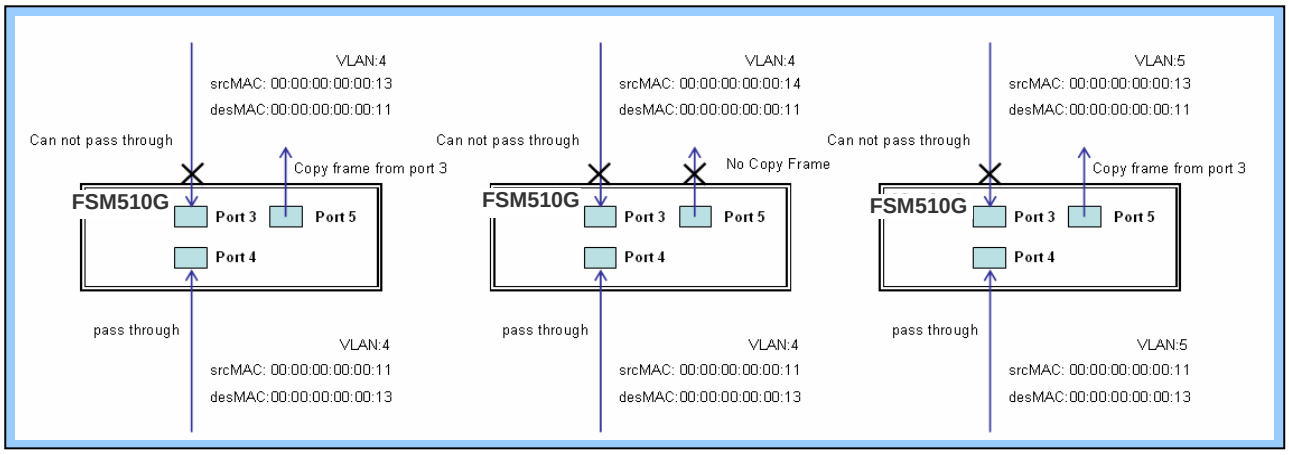


Step 3: Bind this ACL profile to a GE port. (PORT-3)

Step 4: Set analyzer port to enable and mirror analyzer port.



Step 5: Send frames between PORT-3 and PORT-4, see test result.



CLI Command:

```
access-list ace 5 next 6 ingress interface GigabitEthernet 1/3 policy 5 frametype etype smac
00-00-00-00-00-13 dmac 00-00-00-00-00-11
Exit
monitor destination interface GigabitEthernet 1/5
monitor source cpu both
exit
interface GigabitEthernet 1/3
  switchport trunk allowed vlan 4,5
  switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
  switchport trunk allowed vlan 4,5
  switchport trunk vlan tag native
exit
```

Case 2: ACL for IP address

For IP address ACL, it can filter on source IP address, destination IP address, or both. It also supports to set IP range ACL. When it filters on both IP address, packets coincident with both rules will take effect. In other words, it does not do filter if it only coincident with one rule.

If user want to filter only one directional IP address, the other IP address just set to all zero. It means don't care portion. Besides IP address, it also supports Protocol for filter additionally. (TCP=6, UDP=17, etc.) Certain Protocol under these IP addresses will take effect. If user doesn't care Protocol, he can just set to zero value. The detail testing, please refer to MAC ACL above.

Case 3: ACL for L4 Port

For Layer4 port ACL, it can filter on (1) source IP address, (2) source L4 port, (3) destination IP address, (4) destination L4 port, and (5) UDP or TCP Protocol. User can select to filter on (1)~(4) for all or some specific values, but it should select exact one Protocol from UDP or TCP.

When it filters on both directional IP address and L4 port, packets coincident with both rules will take effect. In other words, it does not do filter if it only coincident with one rule.

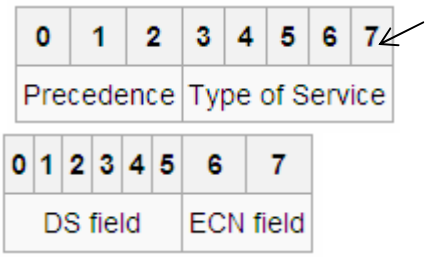
If user wants to filter only one directional IP address or L4 port, the other IP address and L4 port just set to all zero. It means don't care portion. The detail testing, please refer to MAC ACL above.

Case 4: ACL for ToS

For Type of Service (ToS) ACL, it can filter on (1) source IP address with ToS type , or (2) destination IP address with ToS type, or (3) both, or (4) both not (just filter ToS). When it filters on both IP address, packets coincident with both rules will take effect. In other words, it does not do filter if it only coincident with one rule.

If user want to filter only one directional IP address, the other IP address just set to all zero. It means don't care portion. The detail testing, please refer to case 1 MAC ACL above.

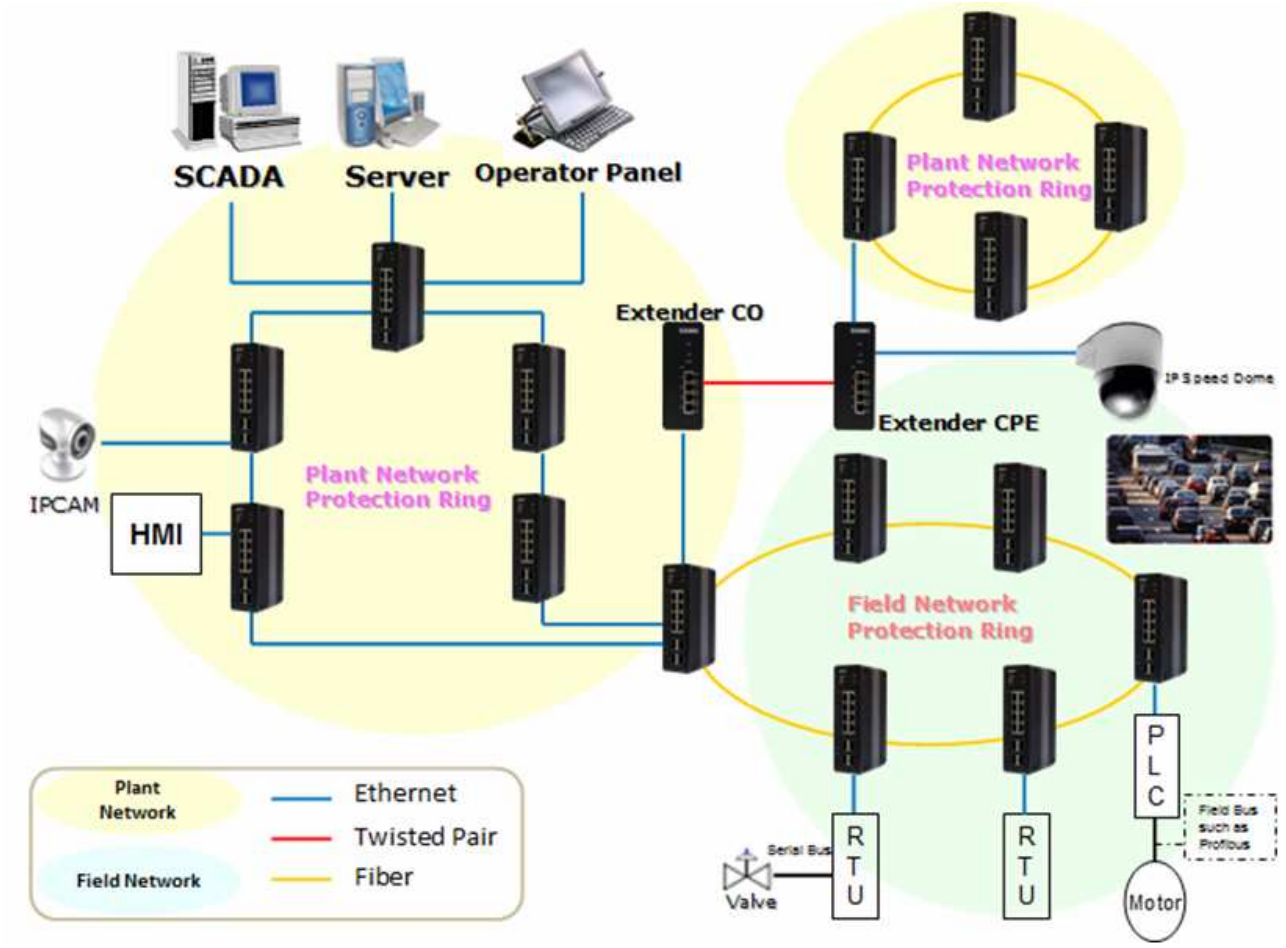
Valid Values: Precedence: 0~7, ToS: 0~15, DSCP: 0~63



This value (7) is reserved and set to 0.
Ex: Pre (001) means 1
Pre (100) means 4
ToS (00010) means 1
ToS (10000) means 8
DSCP (000001) means 1
DSCP (100000) means 32

Ring Version 2 Application Guide

To have a reliable network is very important to Ethernet applications, especially in Industrial domain. Tailyn's FSM-510G provides a mini-second grade failover ring protection; this feature offers a seamless working network even if encountering some matters with connections. It is able to be applied by Ethernet cable and Fiber.



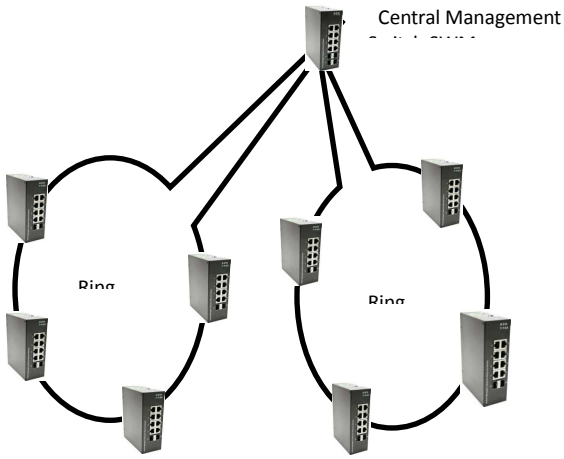
Ring Version 2 Feature

Group 1 - It support option of ring-master and ring-slave.

Ring - it could be master or slave.

When role is ring/master, one ring port is forward port and another is block port. The block port is redundant port. It is blocked in normal state.

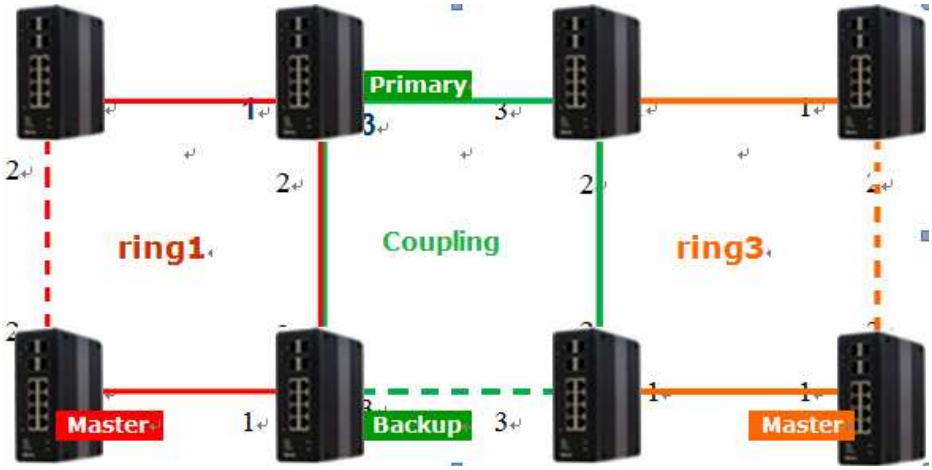
When role is ring/slave, both ring ports are forward port.



Group 2 - It support configuration of the ring, coupling and dual-homing.

Ring - it could be master or slave.

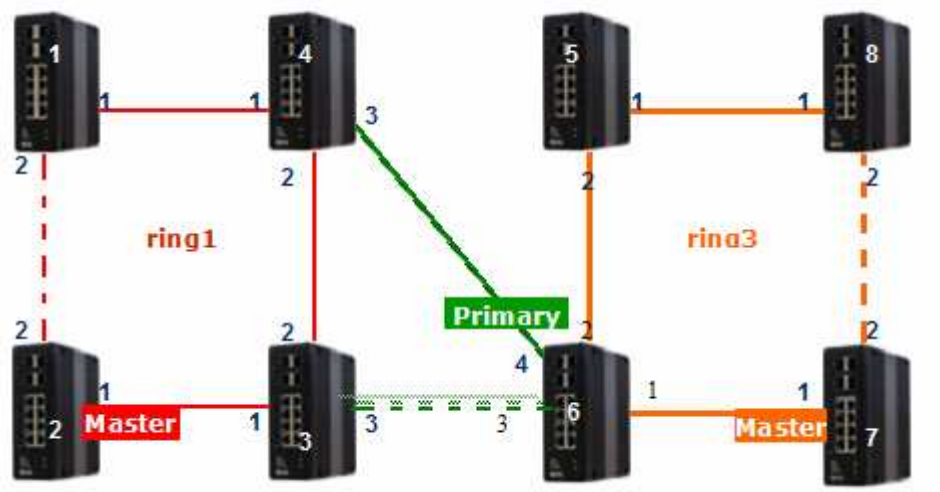
 # Coupling - it could be primary and backup.



When role is coupling/primary, only it need configure one ring port named primary port.

When role is coupling/backup, only it need configure one ring port named backup port. This backup port is redundant port. In normal state, it is blocked.

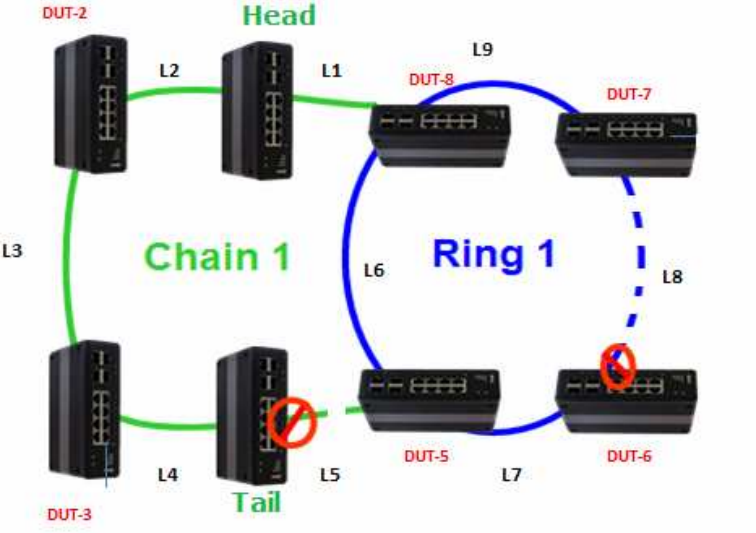
 # Dual-Homing



When role is dual-homing, one ring port is primary port and another is backup port. This backup port is redundant port. In normal state, it is blocked.

Group 3 - It support configuration of the chain and balancing-chain.

 # Chain - it could be head, tail or member.

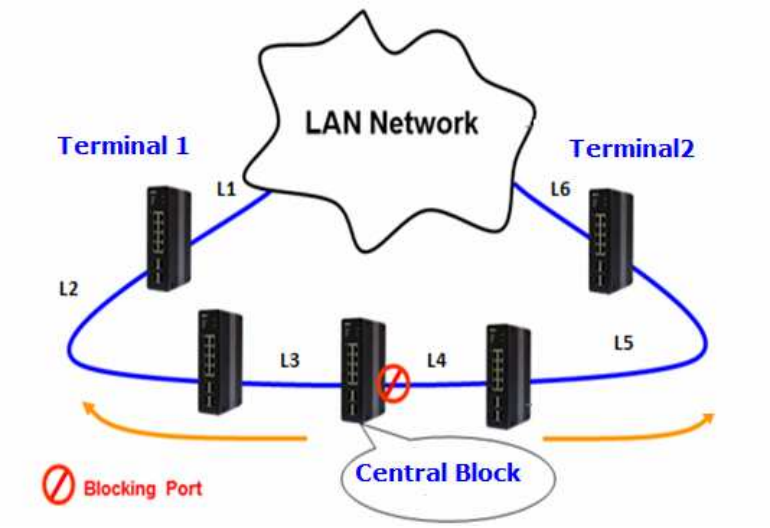


When role is chain/head, one ring port is head port and another is member port. Both ring ports are forwarded in normal state.

When role is chain/tail, one ring port is tail port and another is member port. The tail port is redundant port. It is blocked in normal state.

When role is chain/member, both ring ports are member port. Both ring ports are forwarded in normal state.

 # Balancing Chain - it could be central-block, terminal-1/2 or member.



When role is balancing-chain/central-block, one ring port is member port and another is block port. The block port is redundant port. It is blocked in normal state.

When role is balancing-chain/terminal-1/2, one ring port is terminal port and another is member port. Both ring ports are forwarded in normal state.

When role is balancing-chain/member, both ring ports are member port. Both ring ports are forwarded in normal state.

Note 1 - It must enable group1 before configure group2 as coupling.
Note 2 - When group1 or group2 is enabled, the configuration of group3 is invisible.
Note 3 - When group3 is enabled, the configuration of group1 and group3 is invisible.

How to Configure Ringv2

Configuration (Console)

To configure the ring protection in FSM-510G series management switch,

1. Login "**admin**" account in console
2. Go to Configure mode by "**configure terminal**"
3. Go to configure ring protection group by command "**ringv2 protect group1**"
4. Before configure, must disable ring protection status by by command "**mode disable**"
5. Start to set all necessary parameter:
   - Node 1 and Node 2, choose the ports that you connect with other switch
   - For example, choose PORT-1 and PORT-2 that means PORT-1 is one of the ports connected with other switch, so is PORT-2.
   - Then choose one of ring connection devices be "Master" which you can accept the "Node 2 port" be blocking port.

   id 1
   node1 interface GigabitEthernet 1/1
   node2 interface GigabitEthernet 1/2
   role ring-master

   - Configure finish, . must enable ring protection status by by command "**mode enable**"

Note: Please pay attention on the status of "Previous Command Result" after every action.

configure terminal
ring protect group1

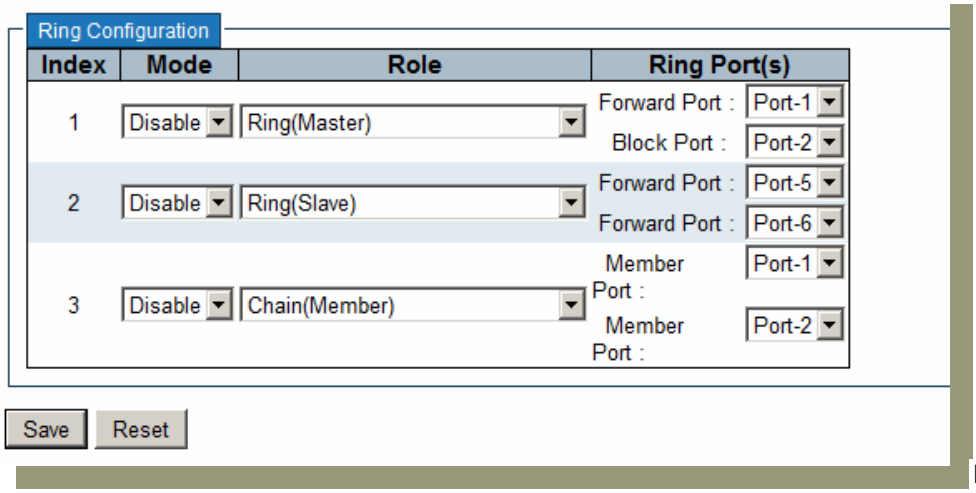
mode disable
node1 interface GigabitEthernet 1/1
node2 interface GigabitEthernet 1/2
role ring-master
mode enable

exit

Configuration (Web UI)

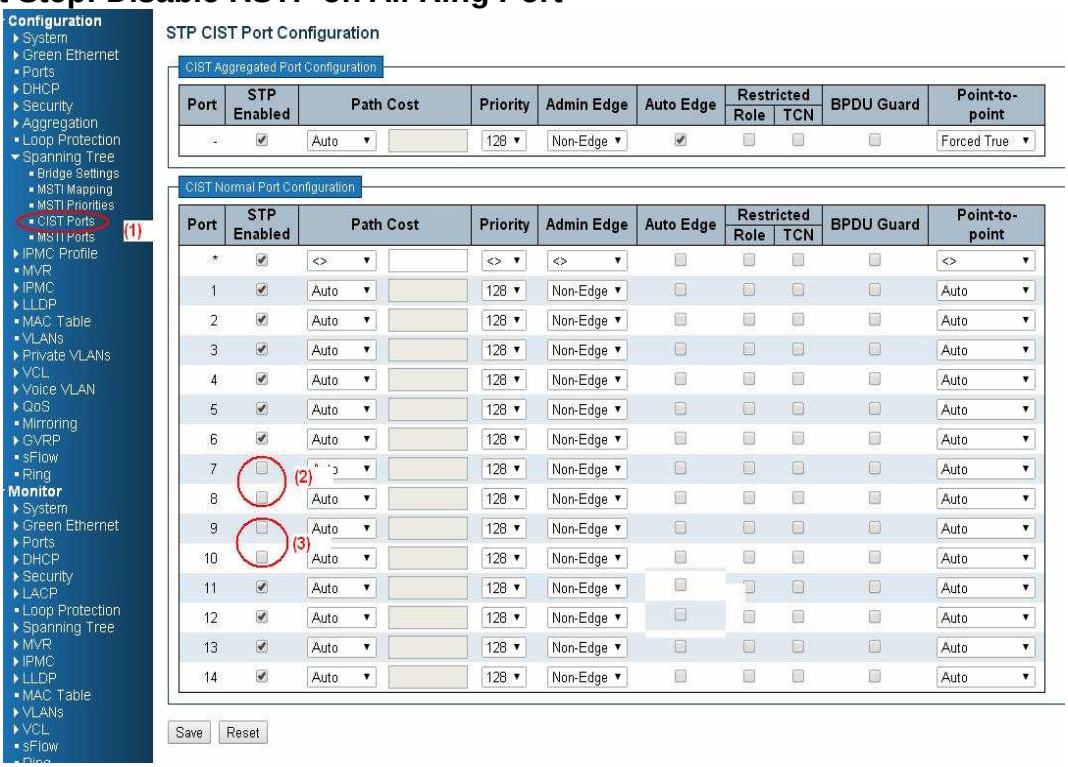
This document is introduction of the Industrial Ethernet Switch Software Spec for Ringv3.

In our current design, one device could support 3 ring index, they are include ring, coupling, dual-homing, chain, and balancing-chain.



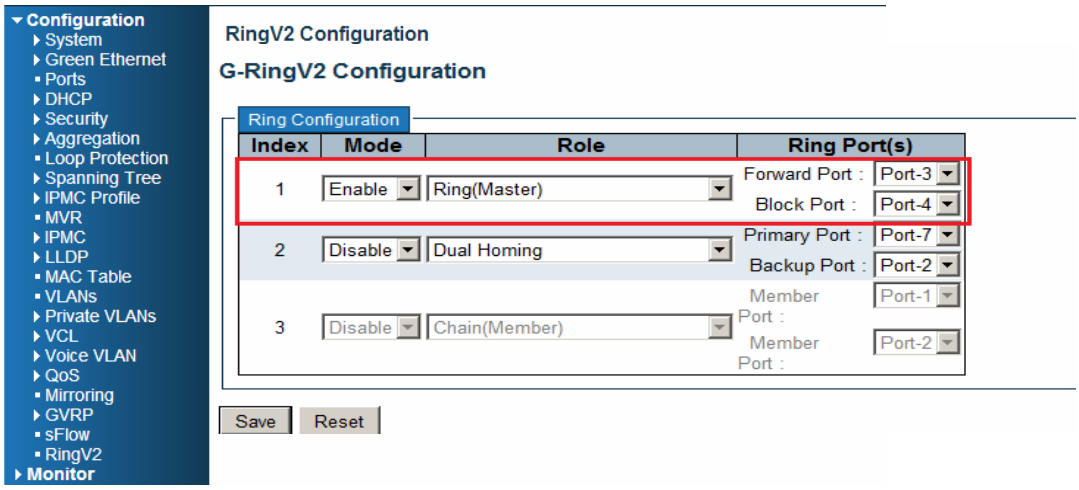
Note 1 - It must enable group1 before configure group2 as coupling.
Note 2 - When group1 or group2 is enabled, the configuration of group3 is invisible.
Note 3 - When group3 is enabled, the configuration of group1 and group3 is invisible.

First Step: Disable RSTP on All Ring Port



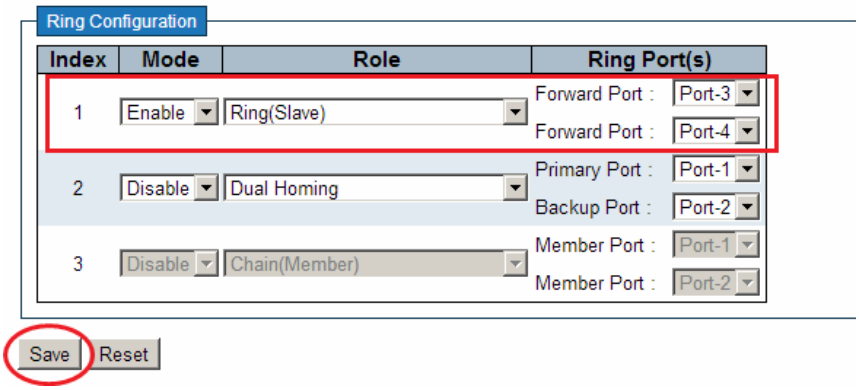
1. Go to "Configuration→Spanning Tree→ CIST ports" Web page
2. Do not enable STP global.
3. Click "Save" bottom

Ring Master



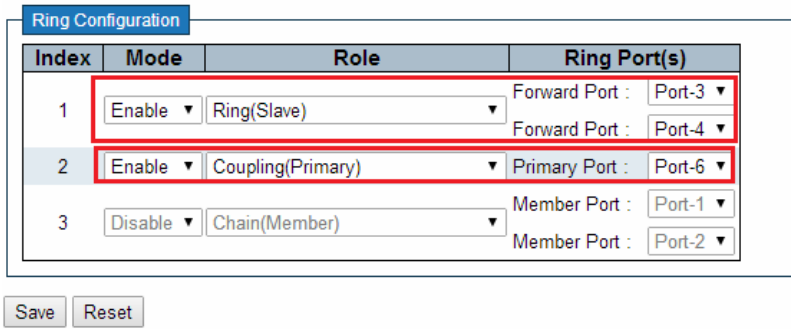
1. Go to “Configuration Ringv2” Web page
2. Enable Group1, and Select Role be “Ring(Master)
3. Select one port link to neighbor devices be “Forward Port”, another is “Block Port”

Ring Slave



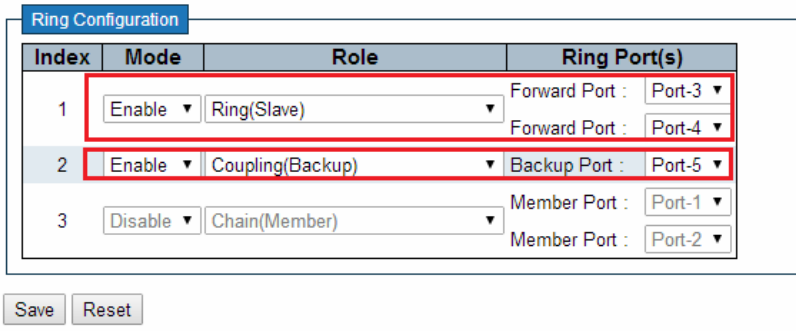
1. Go to “Configuration→Ringv2” Web page
2. Enable Group1, and Select Role be “Ring(Slave)
3. Select two port link to neighbor devices be “Forward Port”.

Coupling Primary



1. Go to “Configuration→Ringv2” Web page
2. Enable Group1, and Select Role be “Ring(Slave)
3. Select two port link to neighbor devices be “Forward Port”.
4. Enable Group2, and Select Role be “Coupling(Primary)”
5. Select one port link to above ring be “Primary Port”.

Coupling Backup

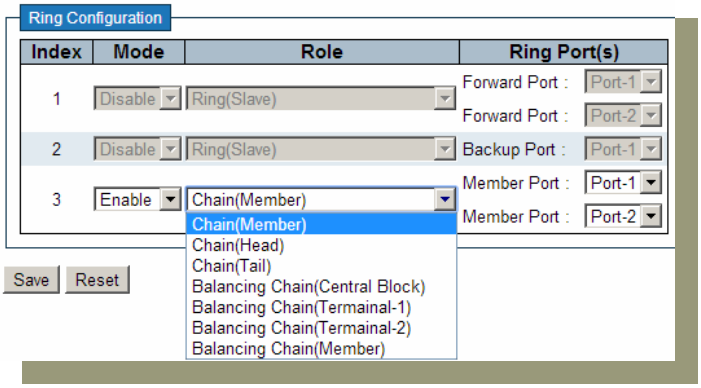


1. Go to “Configuration→Ringv2” Web page
2. Enable Group1, and Select Role be “Ring(Slave)
3. Select two port link to neighbor devices be “Forward Port”.
4. Enable Group2, and Select Role be “Coupling(Backup)”
5. Select one port link to above ring be “Backup Port”.

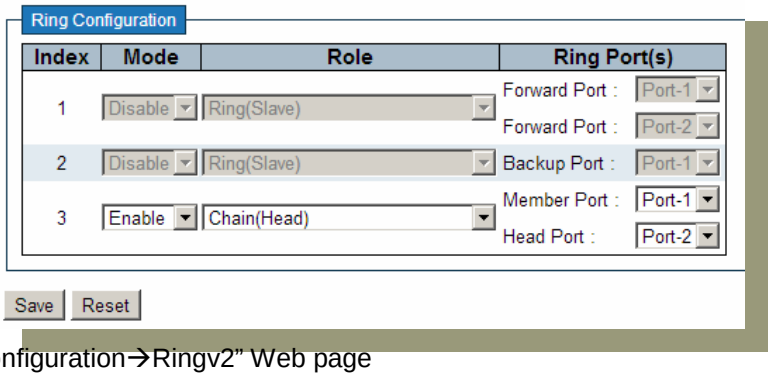
Dual-Homing

1. Go to “Configuration→Ringv2” Web page
2. Enable Group2, and Select Role be “Dual Homing”
3. Select one port link to other ring be “Backup Port”,

Chain(Member)

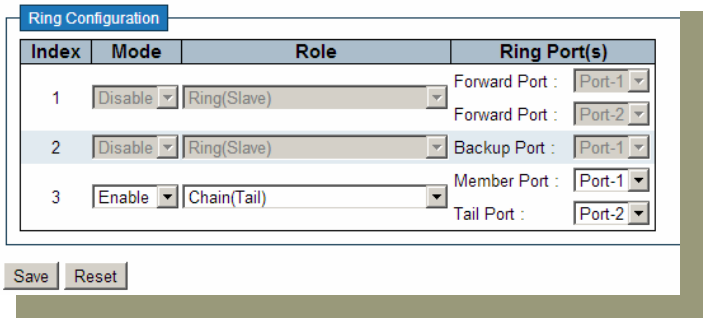


Chain(Haed)



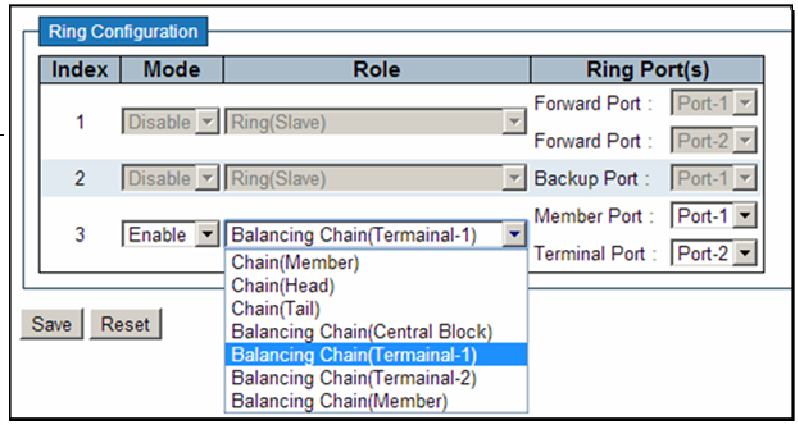
1. Go to “Configuration→Ringv2” Web page
2. Enable Group3, and Select Role be “Chain(Head)”
3. Select one port link to other ring or networks be “Head Port”.

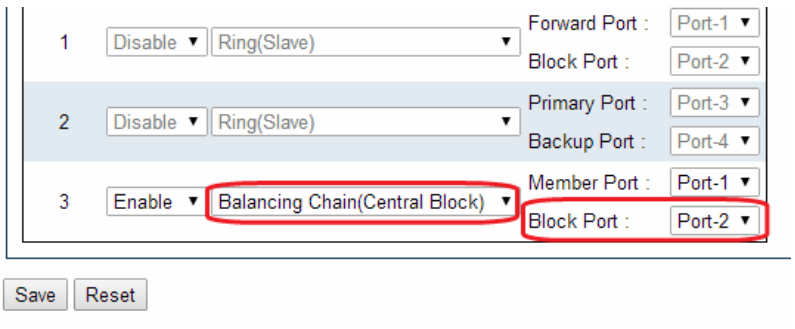
Chain(Tail)



1. Go to “Configuration→Ringv2” Web page
2. Enable Group3, and Select Role be “Chain(Head)”
3. Select one port link to other ring or networks be “Head Port”.

Balance Chain(Central Block)





1. Go to “Configuration→Ringv2” Web page
2. Enable Group3, and Select Role be “Balance Chain(Central Block)”
3. Select one port be “Block Port” which could distribute traffic loading

Balance Chain(Terminal)

1. Go to “Configuration→Ringv2” Web page
2. Enable Group3, and Select Role be “Balance Chain(Terminal-1(or2))”
3. Select one port be “Terminal Port” which connect to other ring group.

QoS Application Guide

Quality of Service (QoS) features allow you to allocate network resources to mission-critical applications at the expense of applications that are less sensitive to such factors as time delays or network congestion. You can configure your network to prioritize specific types of traffic, ensuring that each type receives the appropriate Quality of Service (QoS) level.

SP/SPWRR/WRR

The FSM-510G can be configured to have 8 output Class of Service (CoS) queues (Q0~Q7) per port, into which each packet is placed. Q0 is the highest priority Queue. Each packet's 802.1p priority determines its CoS queue. User needs to bind VLAN priority/queue mapping profile to each port, for every VLAN priority need assign a traffic descriptor for it. The traffic descriptor defines the shapping parameter on every VLAN priority for Ethernet interface. Currently FSM-510G supports Strict Priority (SP)/SPWRR (SP+WRR)/WRR (Weighted Round Robin) scheduling methods on each port. Please find the detail reference on FSM-510G user manual.

Default Priority and Queue mapping as below:

Priority0	Priority1	Priority2	Priority3	Priority4	Priority5	Priority6	Priority7
Queue0	Queue1	Queue2	Queue3	Queue4	Queue5	Queue6	Queue7
WRR	WRR	WRR	WRR	SPQ	SPQ	SPQ	SPQ

Application Examples

Following we provide several examples for various QoS combinations and you can configure QoS using the Web-based management system, CLI (Command Line Interface) or SNMP.

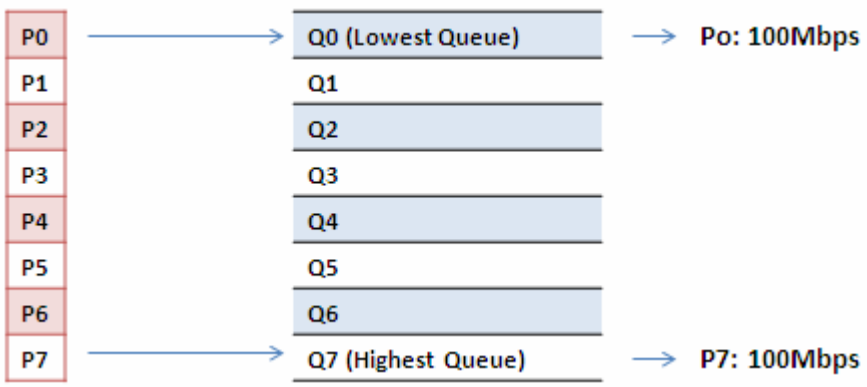
Example 1: SPQ without Shaping (Default profile)

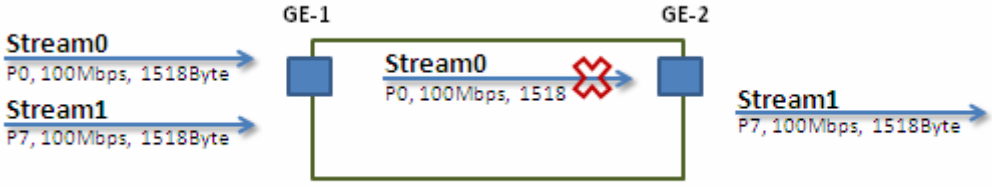
We send 2 Streams (Stream0, Stream1) from PORT-1 to PORT-2. Both 2 Streams each have 100Mbps. Stream0 includes VLAN Priority0, Stream1 includes VLAN Priority7. Set PORT-2 link speed to 100Mbps.

Expected Result:

We expect PORT-2 only can receive 100Mbps of Stream1, and Stream0 will be discarded. This case will help user to know how SPQ works on the FSM-510G.

Gigabit port VLAN Priority & Queue mapping:



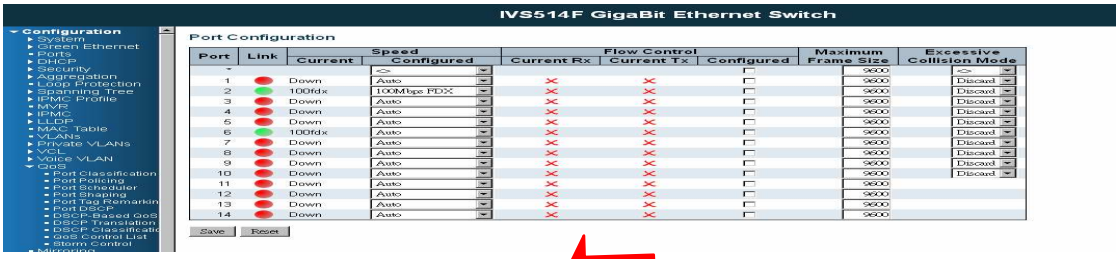


- **Stream0 :**
  Dst Mac : 00:00:00:00:20:01
  Src Mac : 00:00:00:00:10:01
  Vlan : 100
  Vlan prio : 0
  Send rate : 100Mbps
  Packet length: 1518bytes

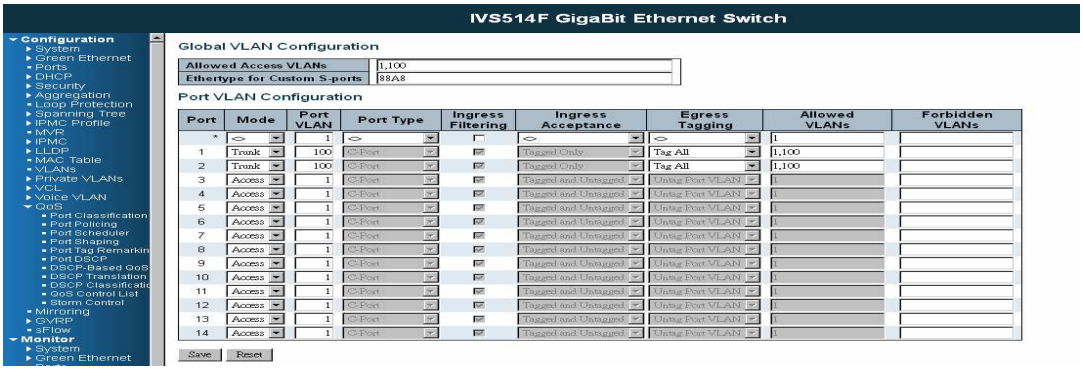
- **Stream1**:
  Dst Mac : 00:00:00:00:20:02
  Src Mac : 00:00:00:00:10:02
  Vlan : 100
  Vlan prio : 7
  Send rate : 100Mbps
  Packet length: 1518bytes

Web management:

Step1. Go to Configuration -> Ports -> set port 2 link speed to 100Mbps full duplex.



Step2. Select Configuration -> VLANs ->Create a VLAN with VLAN ID 100. Enter a VLAN name in the **Name** field. Here we set tagged VLAN100 on PORT-1 and PORT-2.



CLI configuration command:

```
interface GigabitEthernet 1/2
speed 100
duplex full
exit
vlan 100
```

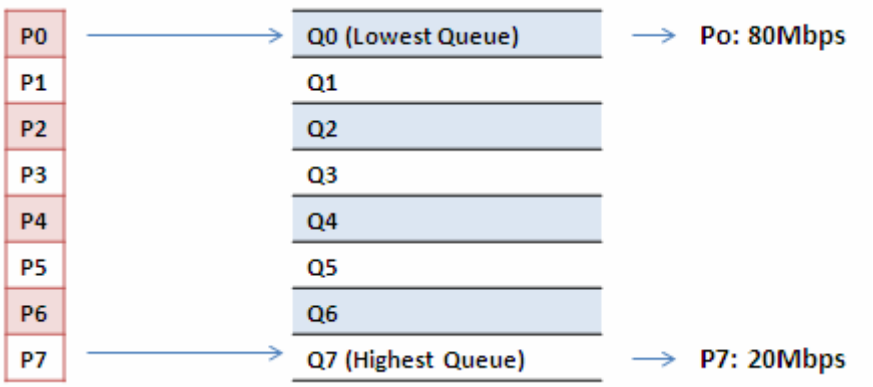
Example 2: SPQ with Shaping

We send 2 Streams (Stream0, Stream1) from port1 to port-2. Both 2 Streams each have 100Mbps. Stream0 includes VLAN Priority0, Stream1 includes VLAN Priority7. Stream3 and Stream4 only for learning which make sure the traffic are not flooding.

Expected Result:

We expect PORT-2 only can receive 20Mbps of Stream1, and 80Mbps of Stream0. This case will help user to know how SPQ works on the FSM-510G.

VDSL port VLAN Priority & Queue mapping:



- **Stream0 :**
  Dst Mac : 00:00:00:00:20:01
  Src Mac : 00:00:00:00:10:01
  Vlan : 100
  Vlan prio : 0
  Send rate : 100Mbps
  Packet length: 1518bytes

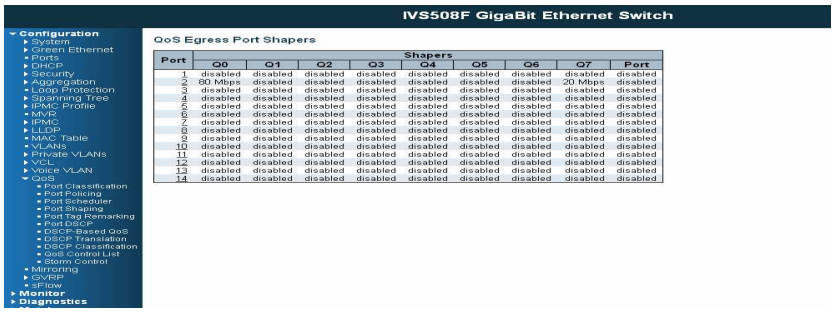
- **Stream1**:
  Dst Mac : 00:00:00:00:20:02
  Src Mac : 00:00:00:00:10:02
  Vlan : 100
  Vlan prio : 7
  Send rate : 100Mbps
  Packet length: 1518bytes

- **Stream3 : (for Learning)**
  Dst Mac : 00:00:00:00:10:01
  Src Mac : 00:00:00:00:20:01
  Vlan : 100
  Vlan prio : 0
  Send rate : 10Mbps
  Packet length: 1518bytes

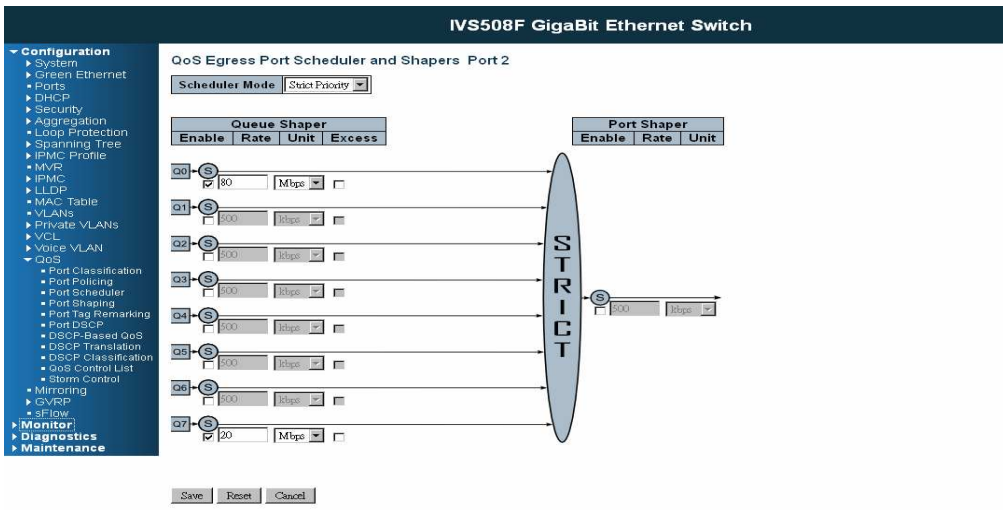
- **Stream4 : (for Learning)**
  Dst Mac : 00:00:00:00:10:02
  Src Mac : 00:00:00:00:20:02
  Vlan : 100
  Vlan prio : 0
  Send rate : 10Mbps
  Packet length: 1518bytes

Web management:

Step1. Go to Configuration -> Qos→ Port Shaping, to create a Qos profile on Port-2.



Step2. Select schedule mode be “”Strict Priority” and set shaping rate for queue 0 and queue 7 as below.



CLI configuration command:

```
vlan 100 v100
interface gigabit 1
vlan 100 tag
exit
interface gigabit 2
qos shaper 100000
qos queue-shaper queue 0 80000
qos queue-shaper queue 7 20000
exit
```

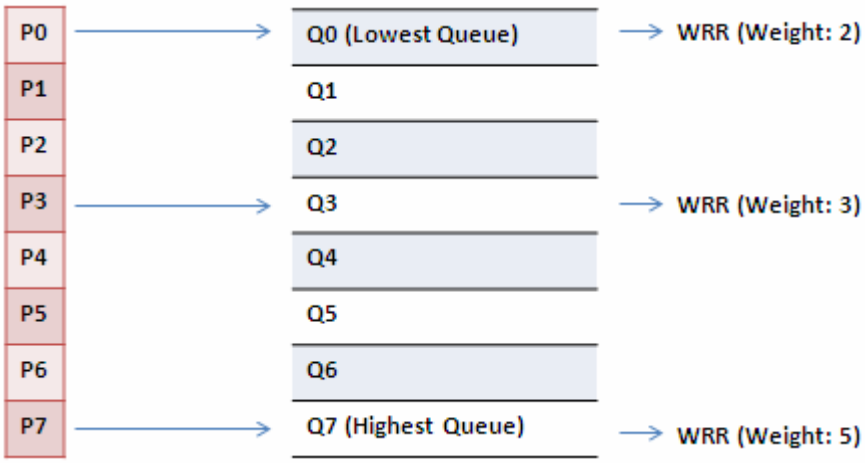
Example 3: WRR

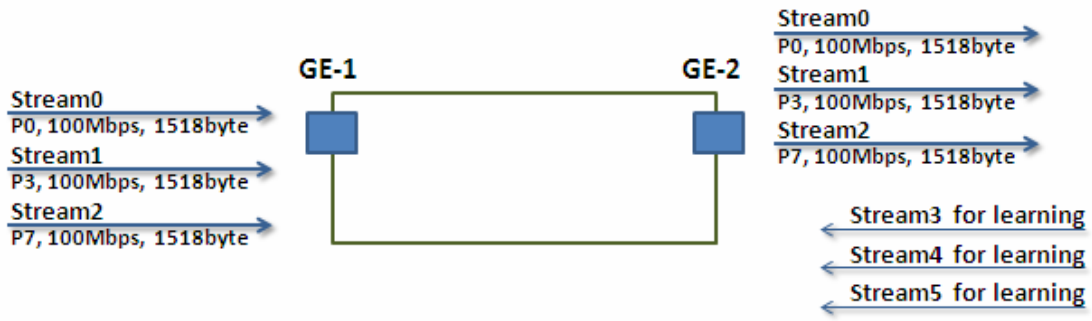
We send 3 Streams (Stream0, Stream1 and Stream2) from PORT-1 to PORT-2. These Streams each have 100Mbps. Stream0 includes VLAN Priority0, Stream1 includes VLAN Priority3, Stream2 includes VLAN Priority7. Stream3, Stream4 and Stream5 only for learning which make sure the traffic are not flooding. WRR support weight assignment, the range of weight value is from 1 to 255. Bye the way, FSM-510G applies WRR scheduling and weight 1 for all the Gigabit Ethernet Port. In the following case, we will assign Weight 2 for Priority0, Weight 3 for Priority3 and Weight 5 for Priority7.

Expected Result:

We expect PORT-2 can receive about 20Mbps of Stream0, 30Mbps of Stream1 and 50Mbps of Stream2. This case will help user to know how WRR works on the FSM-510G.

Gigabit port VLAN Priority & Queue mapping:





- **Stream0 :**
  Dst Mac : 00:00:00:00:20:01
  Src Mac : 00:00:00:00:10:01
  Vlan : 100
  Vlan prio : 0
  Send rate : 100Mbps
  Packet length: 1518bytes

- **Stream1**:
  Dst Mac : 00:00:00:00:20:04
  Src Mac : 00:00:00:00:10:04
  Vlan : 100
  Vlan prio : 3
  Send rate : 100Mbps
  Packet length: 1518bytes

- **Stream2**:
  Dst Mac : 00:00:00:00:20:08
  Src Mac : 00:00:00:00:10:08
  Vlan : 100
  Vlan prio : 7
  Send rate : 100Mbps
  Packet length: 1518bytes

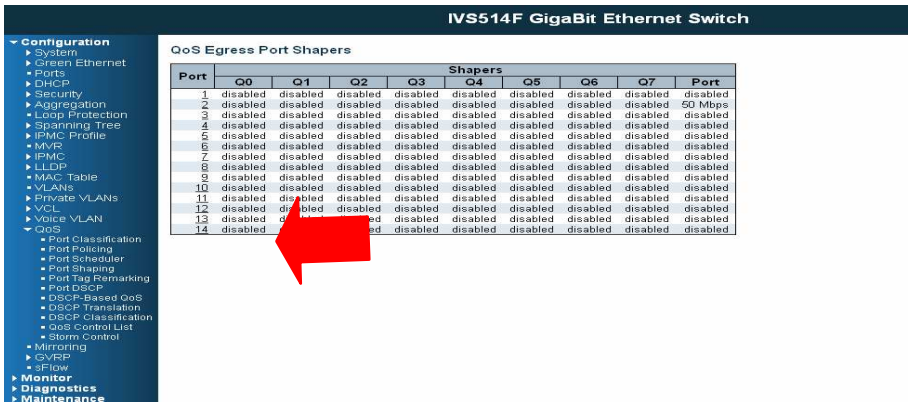
- **Stream3 : (for Learning)**
  Dst Mac : 00:00:00:00:10:01
  Src Mac : 00:00:00:00:20:01
  Vlan : 100
  Vlan prio : 0
  Send rate : 10Mbps
  Packet length: 1518bytes

- **Stream4 : (for Learning)**
  Dst Mac : 00:00:00:00:10:04
  Src Mac : 00:00:00:00:20:04
  Vlan : 100
  Vlan prio : 0
  Send rate : 10Mbps
  Packet length: 1518bytes

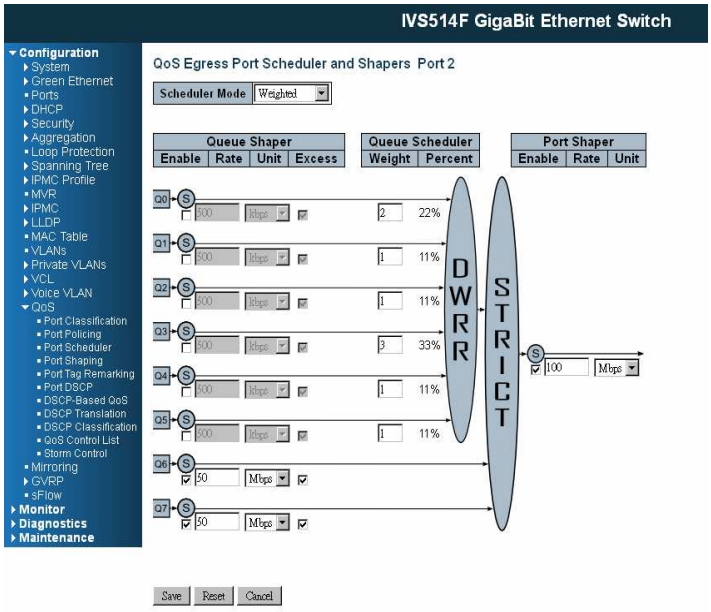
- **Stream5 : (for Learning)**
  Dst Mac : 00:00:00:00:10:08
  Src Mac : 00:00:00:00:20:08
  Vlan : 100
  Vlan prio : 0
  Send rate : 10Mbps
  Packet length: 1518bytes

Web management:

Step1. Go to Configuration -> Qos -> Port shaping, and click on PORT-2 to create a Qos profile.



Step2. Select schedule mode be “”Weighted” and set weight value for queue 0, queue 3 and queue 7 as below.



CLI configuration command:

```
interface GigabitEthernet 1/1
switchport trunk allowed vlan 1,100
switchport hybrid allowed vlan 1,100
switchport trunk vlan tag native
switchport mode trunk
exit
interface GigabitEthernet 1/2
switchport trunk allowed vlan 1,100
switchport trunk vlan tag native
switchport mode trunk
qos shaper 100000
qos queue-shaper queue 6 50000 excess
qos queue-shaper queue 7 50000 excess
qos wrr 2 1 1 3 1 1
exit
```

Example 4 SP-WRR

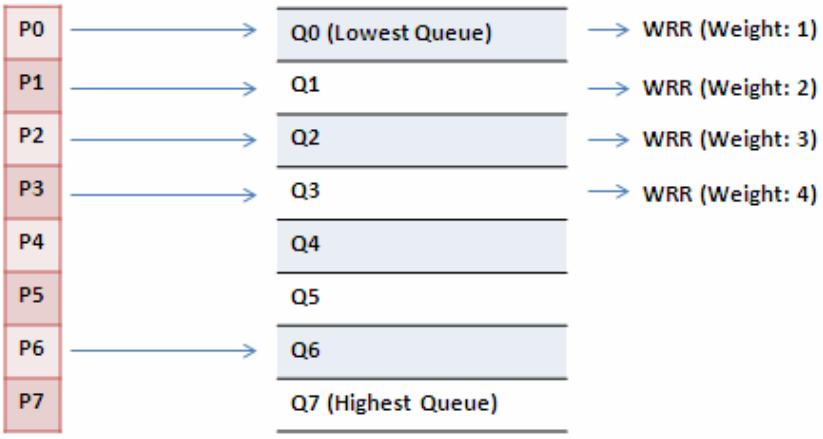
We send 4 Streams (Stream0, Stream1, Stream2 and Stream3) from PORT-1 to PORT-2. These Streams each have 100Mbps. Stream0 includes VLAN Priority0, Stream1 includes VLAN Priority1, Stream2 includes VLAN Priority2, Stream3 includes VLAN Priority3 and Stream4 includes VLAN Priority6. Stream5, Stream6, Stream7, Stream8 and Stream9 only for learning which make sure the traffic are not flooding. WRR support weight assignment, the range of weight value is from 1 to 255. Bye the way, FSM-510G applies WRR scheduling and weight 1 for all the Gigabit Ethernet Port. In the following case, we will assign Weight 1 for Priority0, Weight 2 for Priority1, Weight3 for Priority2 and Weight4 for Priority 3. In SP-WRR mode, queue0 to queue3 belongs to WRR, queue4 to queue6 belongs to SP.

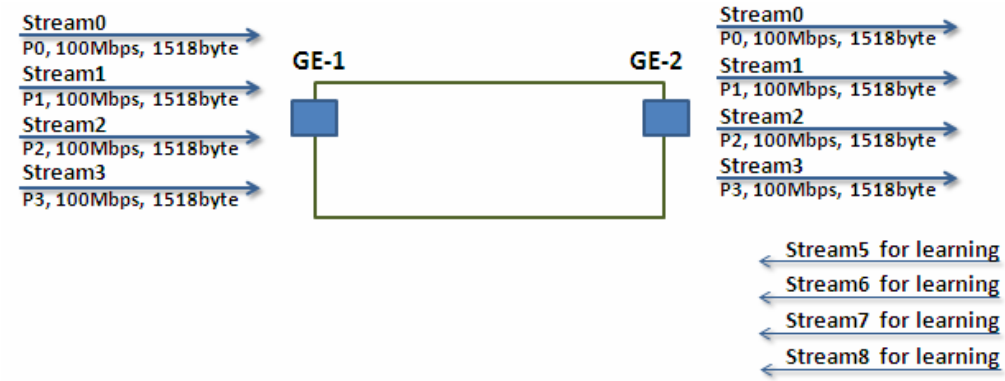
Expected Result:

In Case 1, we expect PORT-2 can receive about 10Mbps of Stream0, 20Mbps of Stream1, 30Mbps of Stream2 and 40Mbps of Stream3 if we send Stream0 to Stream3 to PORT-1. In Case2, we expect PORT-2 only can receive 100Mbps of Stream6, and Stream0 to Stream3 will be discarded in another case. This case will help user to know how SP-WRR works on the FSM-510G.

Case 1:

Gigabit port VLAN Priority & Queue mapping:





- **Stream0 :**
  Dst Mac : 00:00:00:00:20:01
  Src Mac : 00:00:00:00:10:01
  Vlan : 100
  Vlan prio : 0
  Send rate : 100Mbps
  Packet length: 1518bytes

- **Stream1**:
  Dst Mac : 00:00:00:00:20:02
  Src Mac : 00:00:00:00:10:02
  Vlan : 100
  Vlan prio : 3
  Send rate : 100Mbps
  Packet length: 1518bytes

- **Stream2**:
  Dst Mac : 00:00:00:00:20:03
  Src Mac : 00:00:00:00:10:03
  Vlan : 100
  Vlan prio : 7
  Send rate : 100Mbps
  Packet length: 1518bytes

- **Stream3**:
  Dst Mac : 00:00:00:00:20:04
  Src Mac : 00:00:00:00:10:04
  Vlan : 100
  Vlan prio : 7
  Send rate : 100Mbps
  Packet length: 1518bytes

- **Stream5 : (for Learning)**
  Dst Mac : 00:00:00:00:10:01
  Src Mac : 00:00:00:00:20:01
  Vlan : 100
  Vlan prio : 0
  Send rate : 10Mbps
  Packet length: 1518bytes

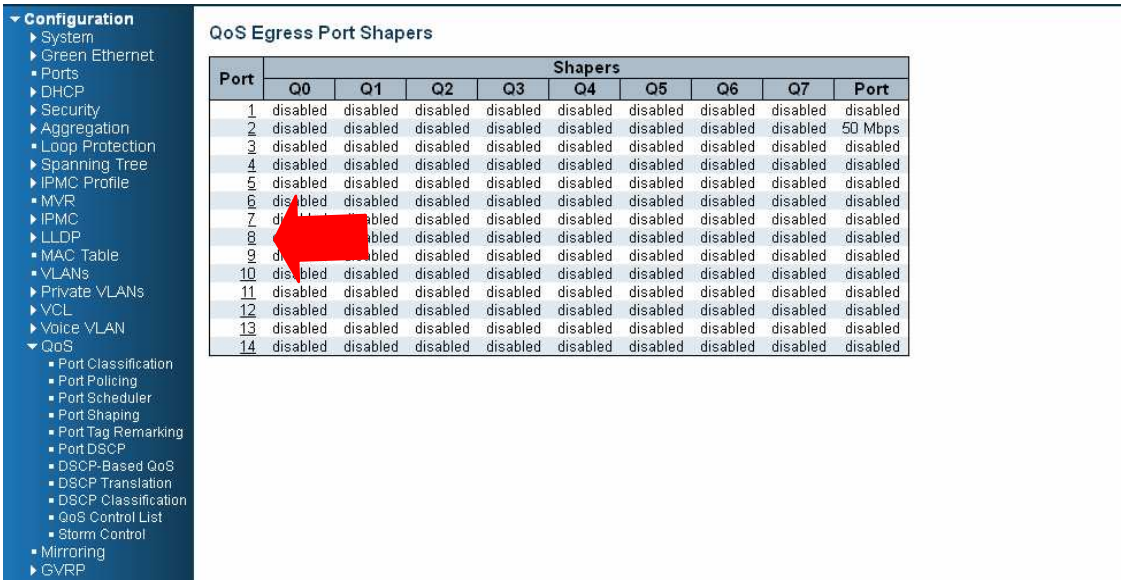
- **Stream6 : (for Learning)**
  Dst Mac : 00:00:00:00:10:02
  Src Mac : 00:00:00:00:20:02
  Vlan : 100
  Vlan prio : 0
  Send rate : 10Mbps
  Packet length: 1518bytes

- **Stream7 : (for Learning)**
  Dst Mac : 00:00:00:00:10:03
  Src Mac : 00:00:00:00:20:03
  Vlan : 100
  Vlan prio : 0
  Send rate : 10Mbps
  Packet length: 1518bytes

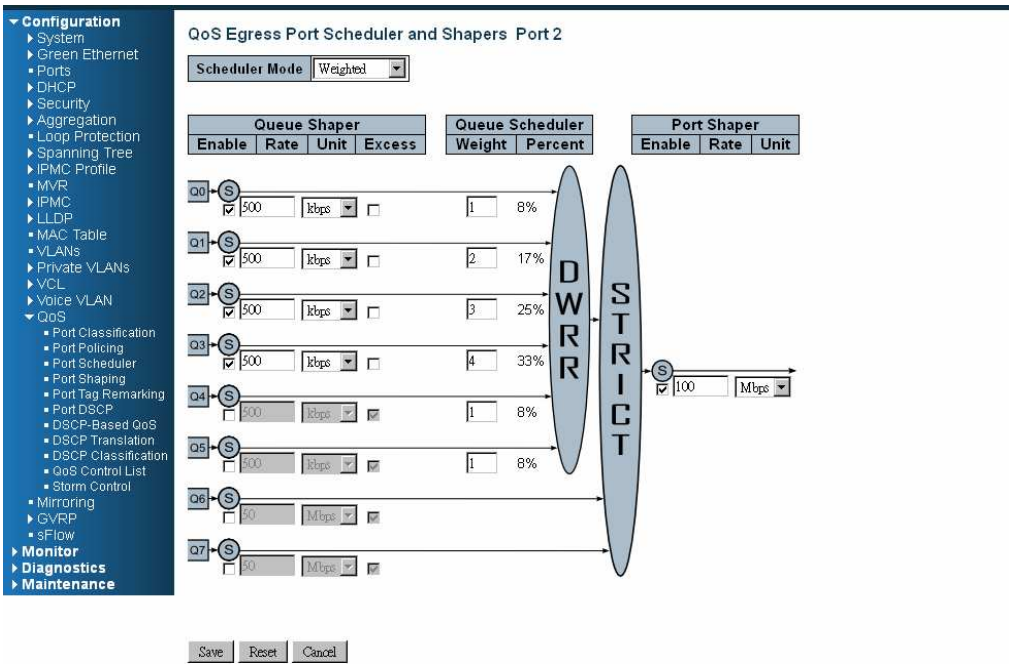
- **Stream8 : (for Learning)**
  Dst Mac : 00:00:00:00:10:04
  Src Mac : 00:00:00:00:20:04
  Vlan : 100
  Vlan prio : 0
  Send rate : 10Mbps
  Packet length: 1518bytes

Web management:

Step1. Go to Configuration -> Qos -> Port shaping, and click on PORT-2 to create a Qos profile.



Step2. Select schedule mode be “”Weighted” and set weight value for queue 0, and set weight value for queue 0~ queue 3 as below.



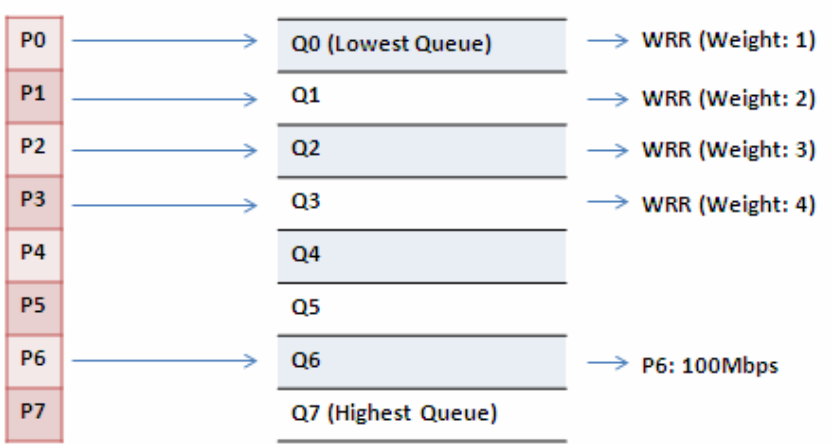
Step2. Go to Configuration-> Queue and Scheduler -> Binding, and bind profile 2 on PORT-2.

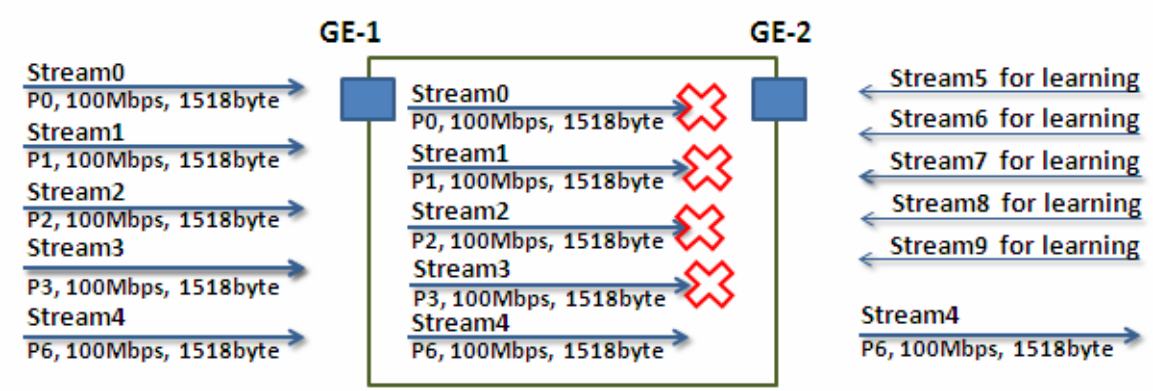
CLI configuration command:

```
interface GigabitEthernet 1/2
  switchport trunk allowed vlan 1,100
  switchport hybrid allowed vlan 100,4095
  switchport trunk vlan tag native
  switchport mode trunk
  qos shaper 100000
  qos queue-shaper queue 0 500
  qos queue-shaper queue 1 500
  qos queue-shaper queue 2 500
  qos queue-shaper queue 3 500
  qos wrr 1 2 3 4 1 1
exit
```

Case 2:

Gigabit port VLAN Priority & Queue mapping





- **Stream0 :**
  Dst Mac : 00:00:00:00:20:01
  Src Mac : 00:00:00:00:10:01
  Vlan : 100
  Vlan prio : 0
  Send rate : 100Mbps
  Packet length: 1518bytes

- **Stream1**:
  Dst Mac : 00:00:00:00:20:02
  Src Mac : 00:00:00:00:10:02
  Vlan : 100
  Vlan prio : 3
  Send rate : 100Mbps
  Packet length: 1518bytes

- **Stream2**:
  Dst Mac : 00:00:00:00:20:03
  Src Mac : 00:00:00:00:10:03
  Vlan : 100
  Vlan prio : 7
  Send rate : 100Mbps
  Packet length: 1518bytes

- **Stream3**:
  Dst Mac : 00:00:00:00:20:04
  Src Mac : 00:00:00:00:10:04
  Vlan : 100
  Vlan prio : 7
  Send rate : 100Mbps
  Packet length: 1518bytes

- **Stream4**:
  Dst Mac : 00:00:00:00:20:07
  Src Mac : 00:00:00:00:10:07
  Vlan : 100
  Vlan prio : 7
  Send rate : 100Mbps
  Packet length: 1518bytes

- **Stream5 : (for Learning)**
  Dst Mac : 00:00:00:00:10:01
  Src Mac : 00:00:00:00:20:01
  Vlan : 100
  Vlan prio : 0
  Send rate : 10Mbps
  Packet length: 1518bytes

- **Stream6 : (for Learning)**
  Dst Mac : 00:00:00:00:10:02
  Src Mac : 00:00:00:00:20:02
  Vlan : 100
  Vlan prio : 0
  Send rate : 10Mbps
  Packet length: 1518bytes

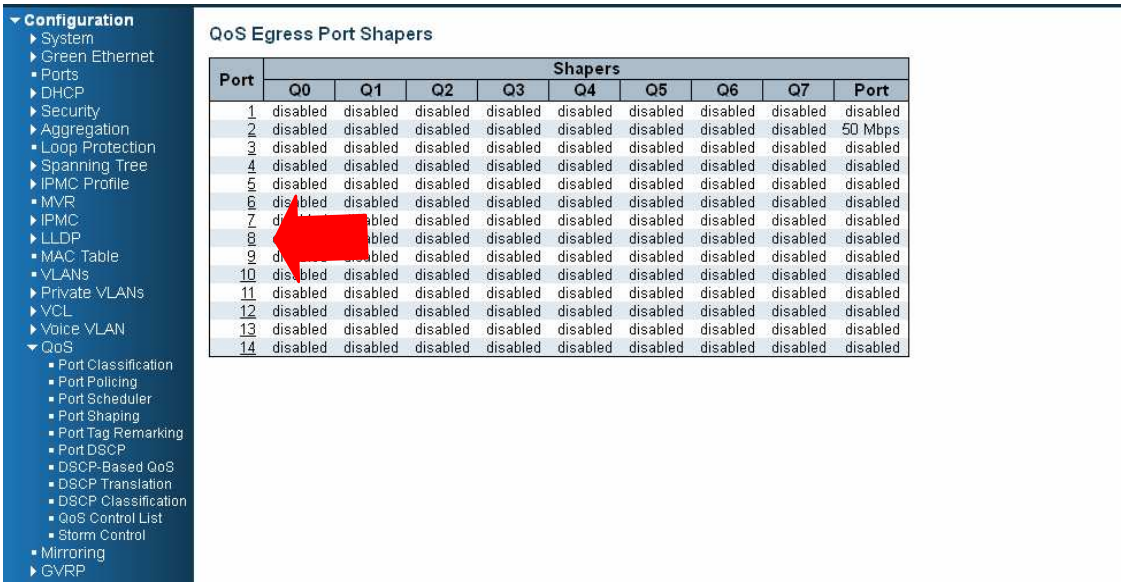
- **Stream7 : (for Learning)**
  Dst Mac : 00:00:00:00:10:03
  Src Mac : 00:00:00:00:20:03
  Vlan : 100
  Vlan prio : 0
  Send rate : 10Mbps
  Packet length: 1518bytes

- **Stream8 : (for Learning)**
  Dst Mac : 00:00:00:00:10:04
  Src Mac : 00:00:00:00:20:04
  Vlan : 100
  Vlan prio : 0
  Send rate : 10Mbps
  Packet length: 1518bytes

- **Stream9 : (for Learning)**
  Dst Mac : 00:00:00:00:10:07
  Src Mac : 00:00:00:00:20:07
  Vlan : 100
  Vlan prio : 0
  Send rate : 10Mbps
  Packet length: 1518bytes

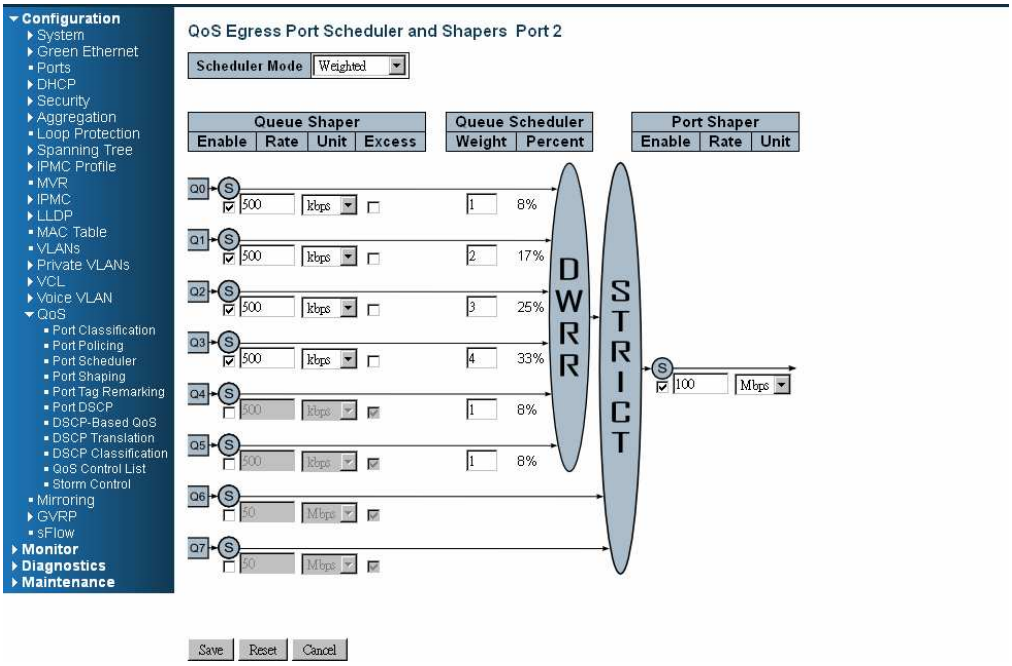
Web management:

Step1. Go to Configuration -> Qos -> Port shaping, and click on PORT-2 to create a Qos profile.



Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	50 Mbps
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
11	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
12	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
13	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
14	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

Step2. Select schedule mode be “”Weighted” and set weight value for queue 0, and set weight value for queue 0~ queue 3 as below.

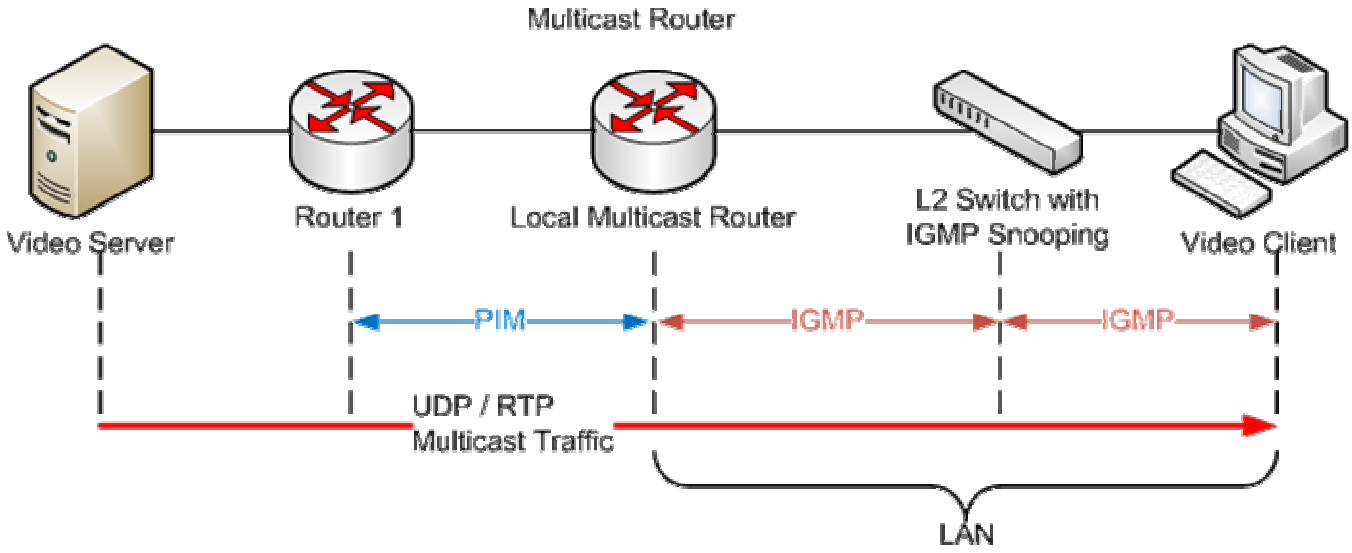


CLI configuration command:

```
interface GigabitEthernet 1/2
  switchport trunk allowed vlan 1,100
  switchport hybrid allowed vlan 100,4095
  switchport trunk vlan tag native
  switchport mode trunk
  qos shaper 100000
  qos wrr 1 2 3 4 1 1
exit
```

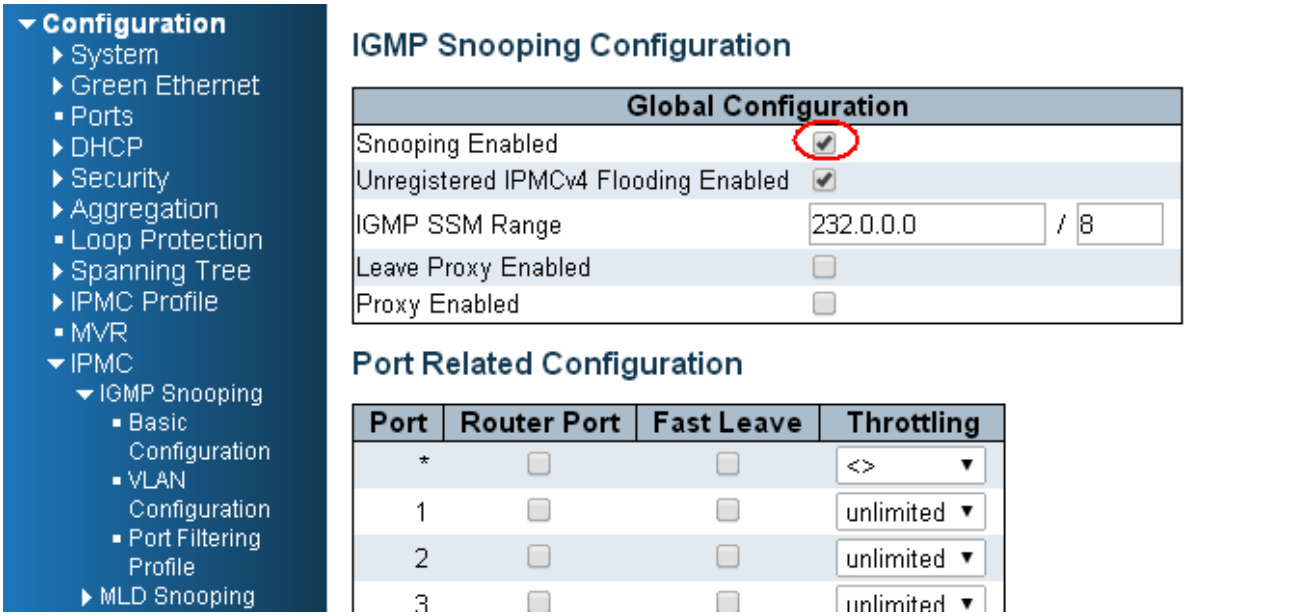
IGMP Application Guide

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

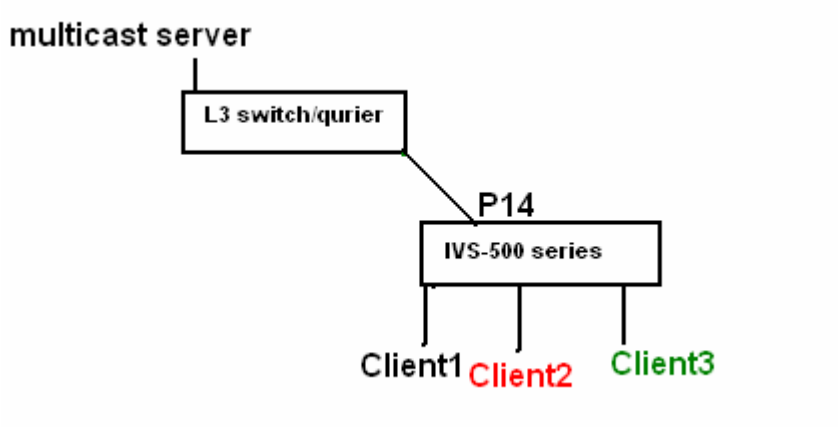


Example 1:

If administrator every client could get multicast stream, just go to “Configuration→IPMC→Bbasic Configuration” to select the check box of “Snooping Enable”, then success.

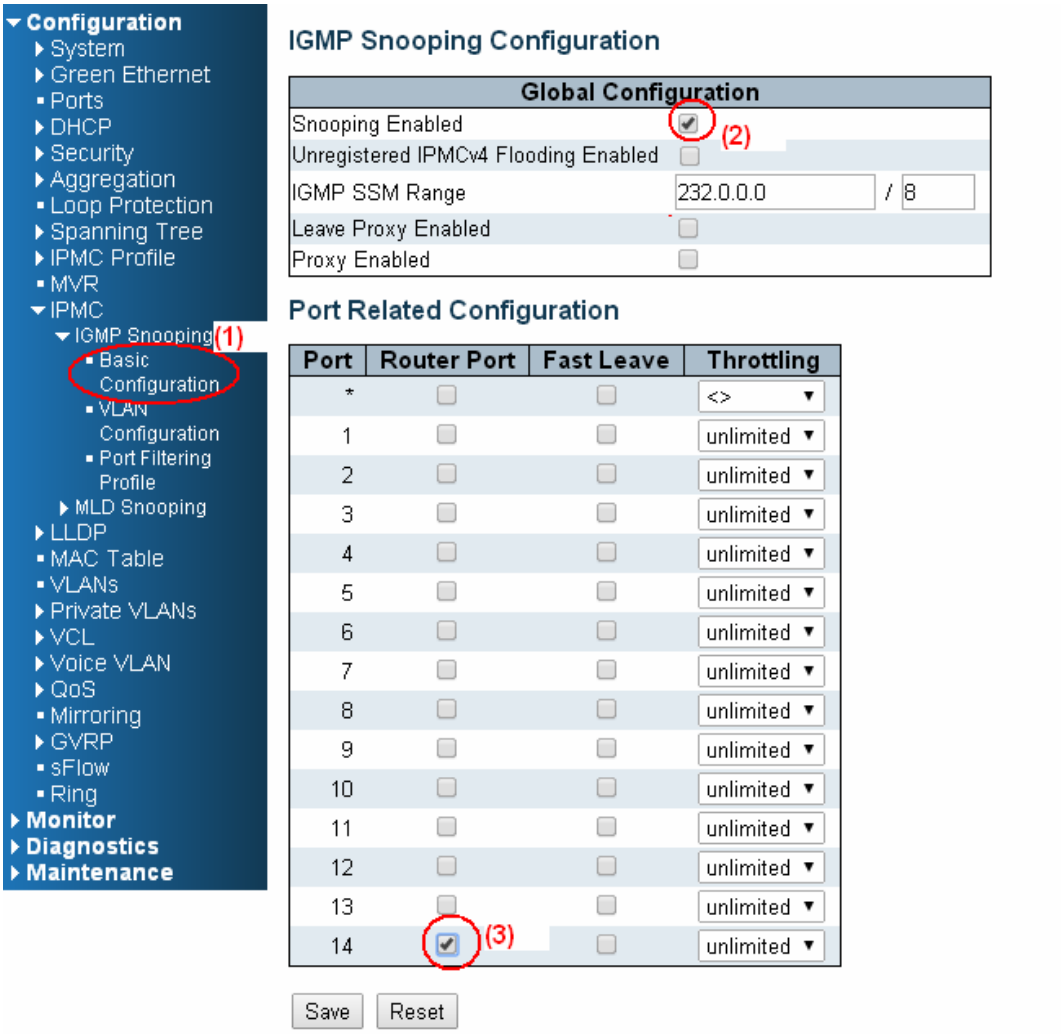

Configuration
System
Green Ethernet
Ports
DHCP
Security
Aggregation
Loop Protection
Spanning Tree
IPMC Profile
MVR
IPMC
IGMP Snooping
Basic Configuration
VLAN Configuration
Port Filtering Profile
MLD Snooping
IGMP Snooping Configuration
Global Configuration
Snooping Enabled
Unregistered IPMCv4 Flooding Enabled
IGMP SSM Range
232.0.0.0
/ 8
Leave Proxy Enabled
Proxy Enabled
Port Related Configuration
Port
Router Port
Fast Leave
Throttling
*
<>
1
unlimited
2
unlimited
3
unlimited

Example2:

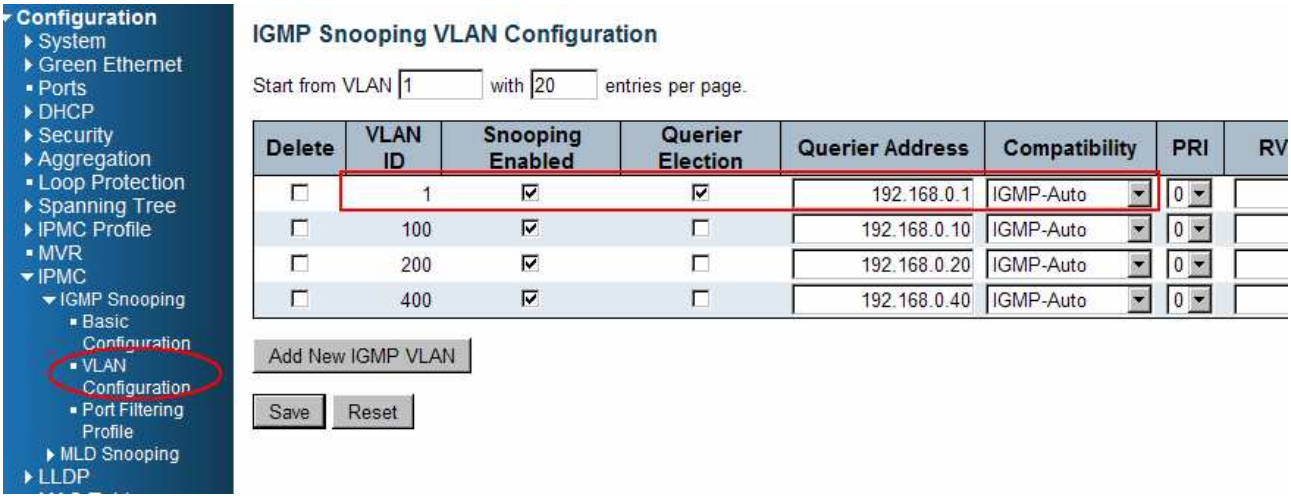


1. Go to “Configuration→IPMC→Basic Configuration” to select the check box of “Snooping Enable”
2. Un-select the check box of ”Unregistered IPMCv4 Flooding Enabled”
3. If Multicast stream is from L3 switch, then the uplink port have to be “Router Port”

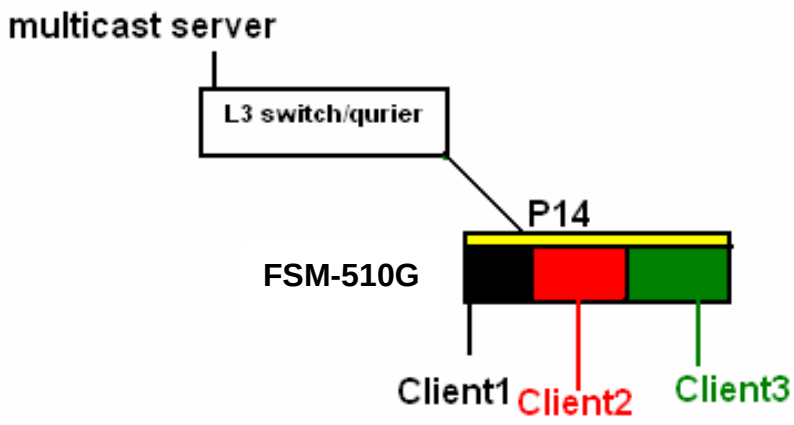
Notice: If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.



(4) Go to “Configuration→IPMC→VLAN Configuration” to select the check box of “Snooping Enable” and set VLAN ID of port14.

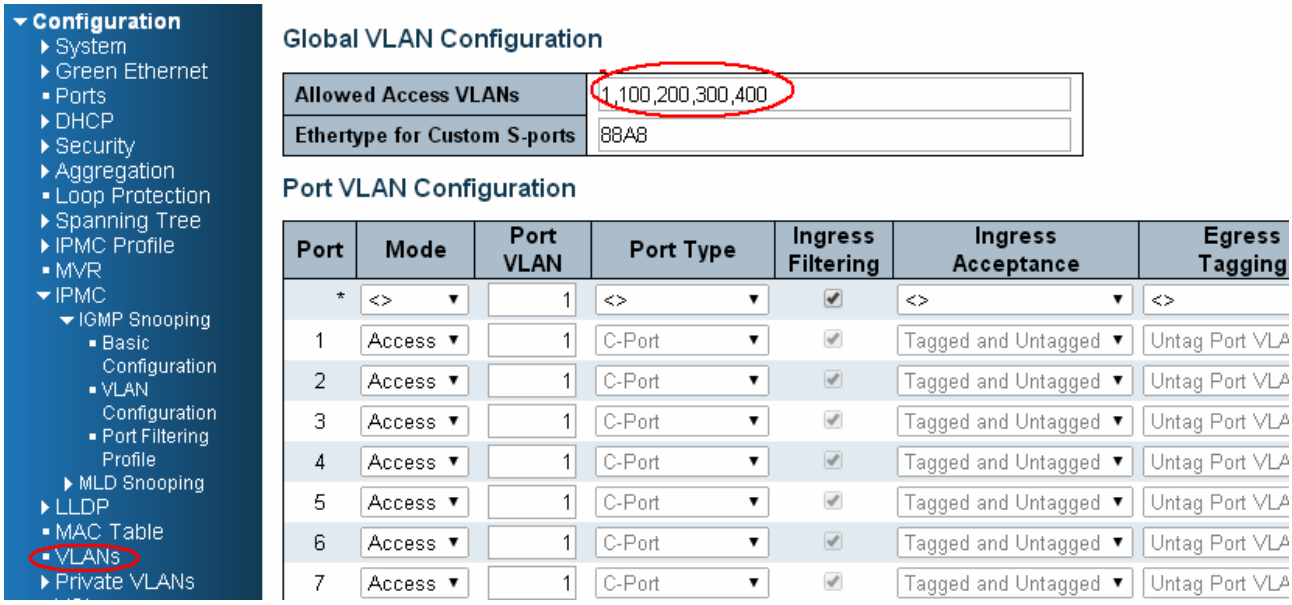

Configuration
System
Green Ethernet
Ports
DHCP
Security
Aggregation
Loop Protection
Spanning Tree
IPMC Profile
MVR
IPMC
IGMP Snooping
Basic Configuration
VLAN Configuration
Port Filtering Profile
MLD Snooping
LLDP
IGMP Snooping VLAN Configuration
Start from VLAN 1 with 20 entries per page.
Delete
VLAN ID
Snooping Enabled
Querier Election
Querier Address
Compatibility
PRI
RV
1
192.168.0.1
IGMP-Auto
100
192.168.0.10
200
192.168.0.20
400
192.168.0.40
Add New IGMP VLAN
Save
Reset

Example3:

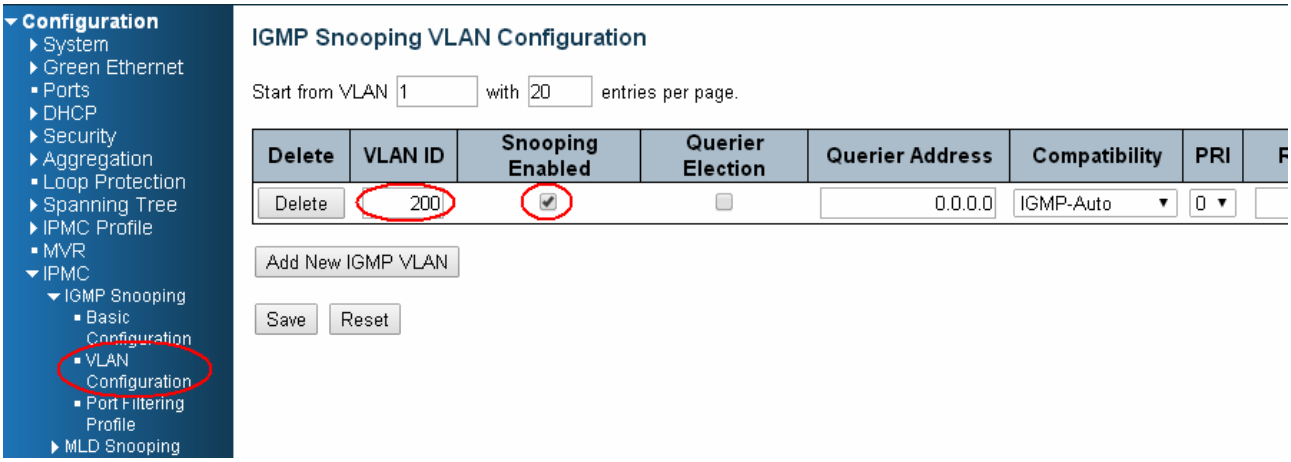


In this scenario, these clients belong to multiple vlans, you have to create more one vlan to be the agent for all client vlans.

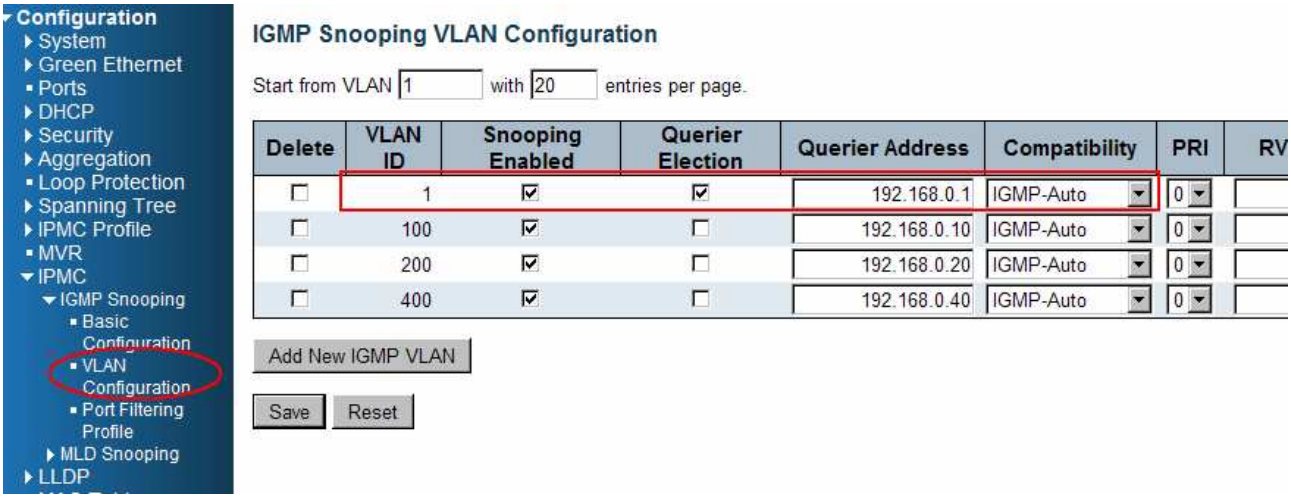
1. To create a vlan : go to ”Configuration→VLANs→Allow Access VLANs”, then set port 14 be vlan200 member port.



2. Go to “Configuration→IPMC→VLAN Configuration” to select the check box of “Snooping Enable” and set VLAN ID of port14.



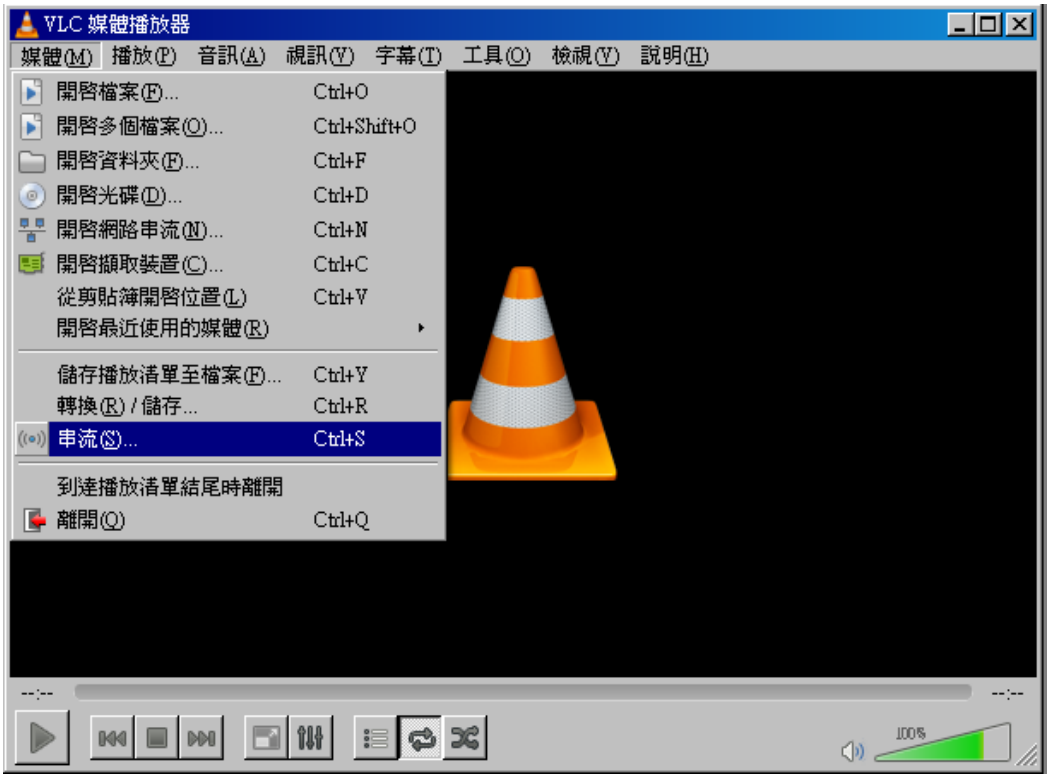
3. If there is no querier on the L3 switch, you have to select “Querier Election”, and set the “Querier Address ”, the IP address is in the same network as uplink interface.
4. Selecet the IGMP version as server.



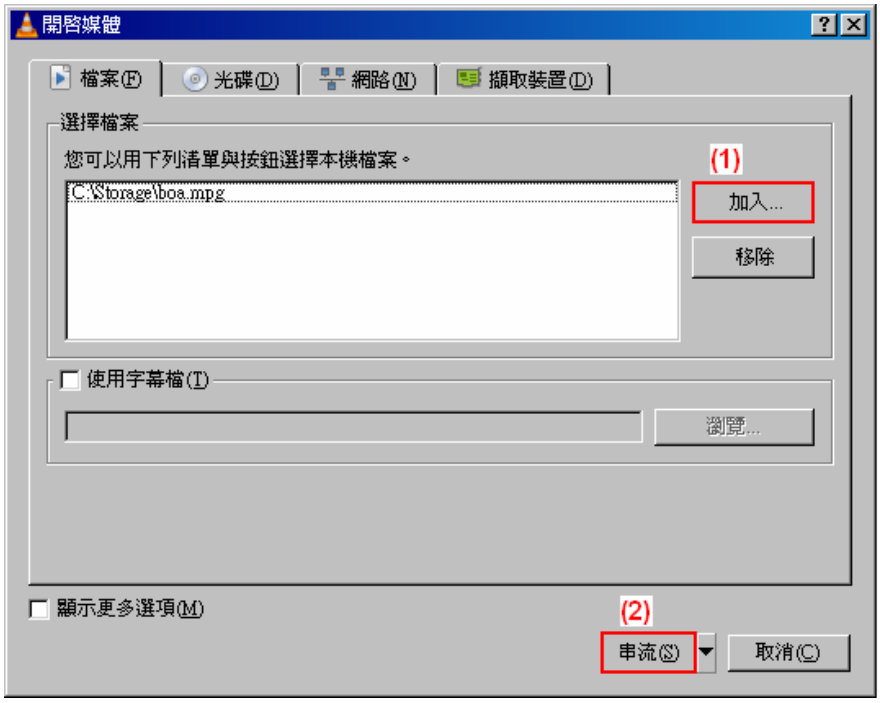
How to Configuration VLC

VLC Configure on IGMP Server

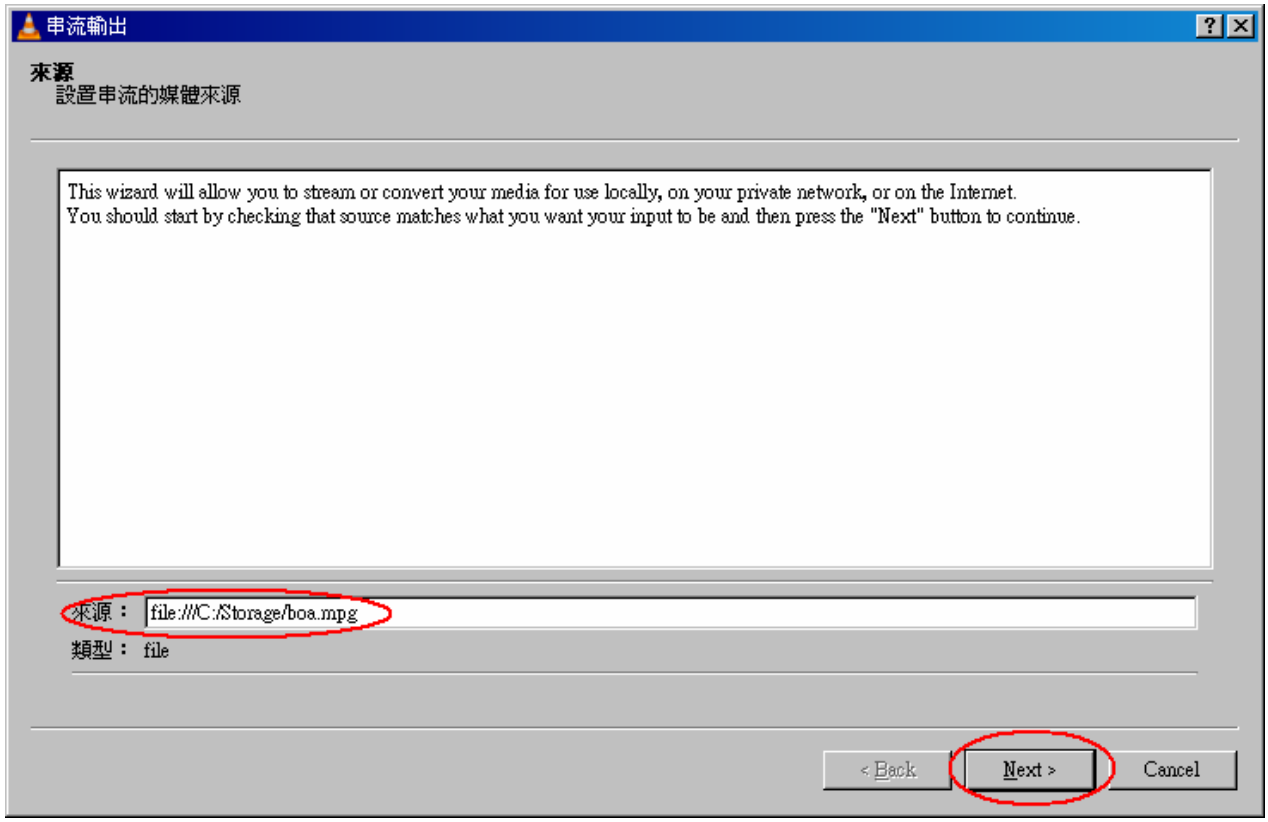
(1) In «Media » area of top tool bar to select “Stream”



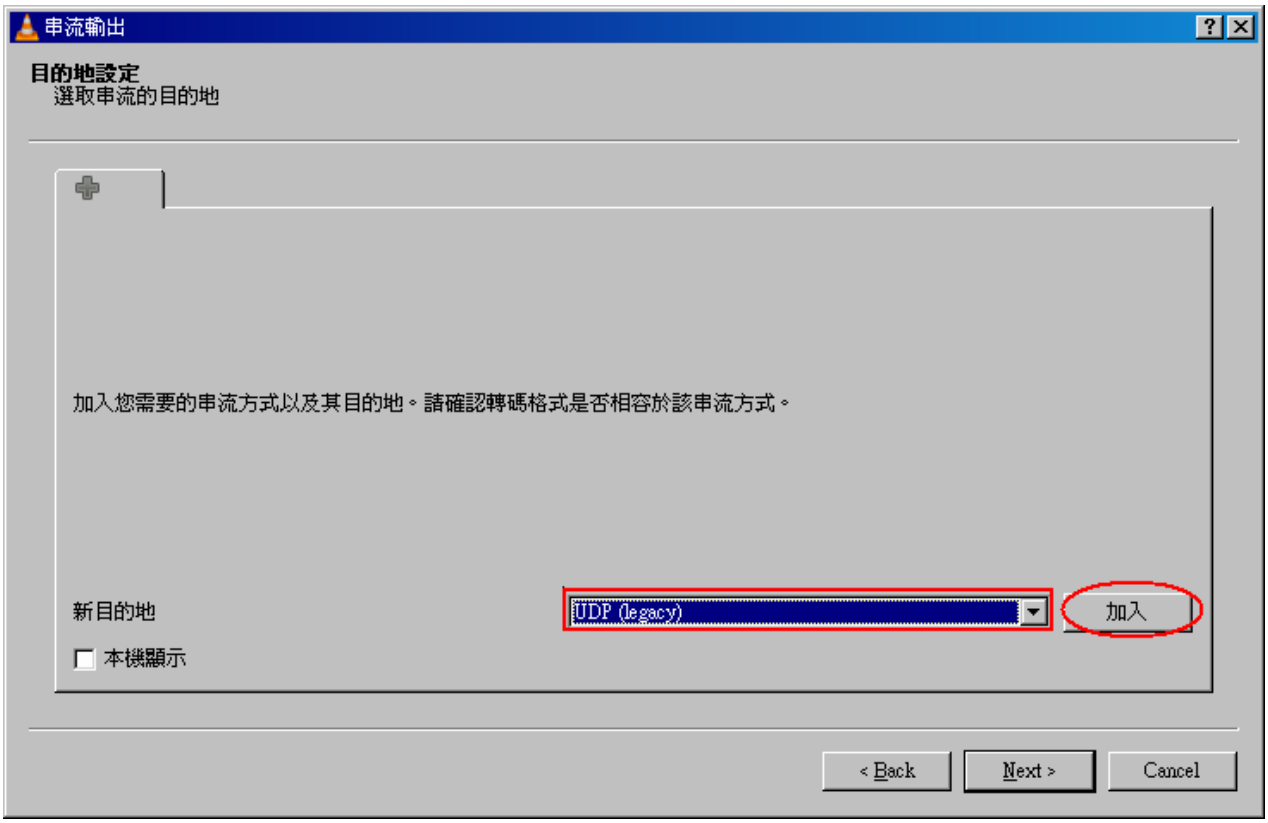
(2) Select a video or voiced file to play



(3) Confirm the file is right, then click “Next” twice.

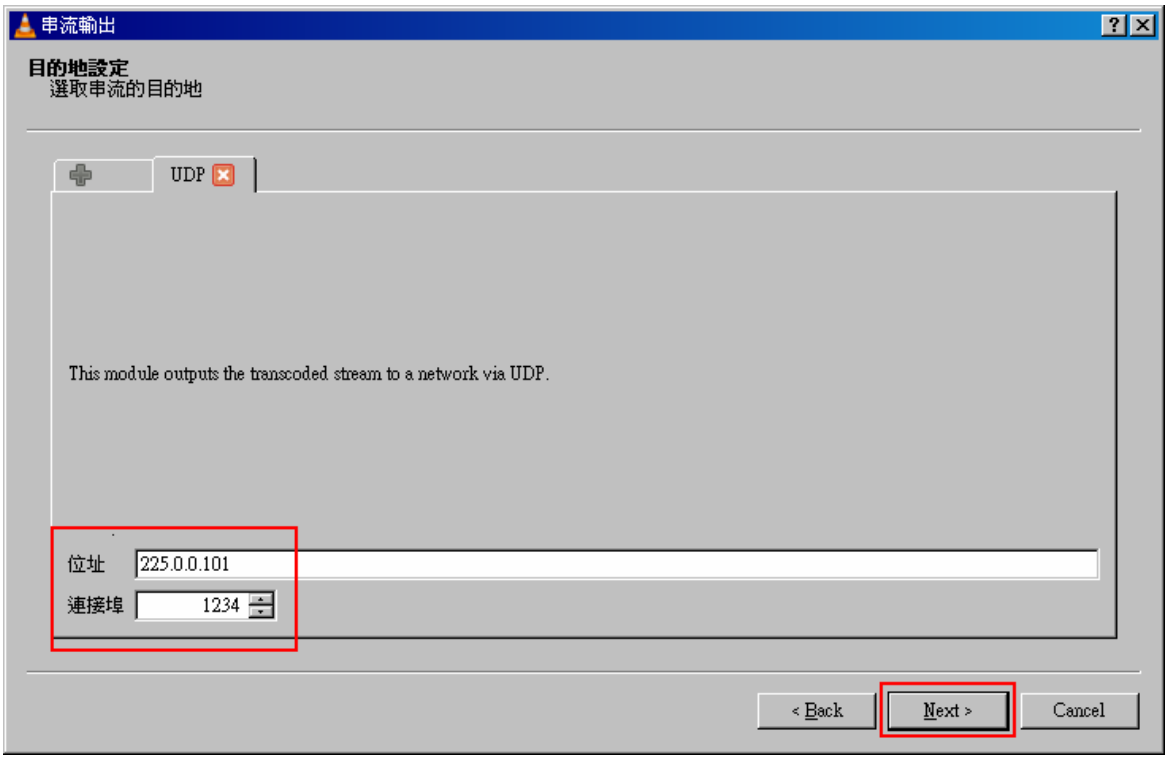


(4) Select stream type as “UDP” and click “Add” button.

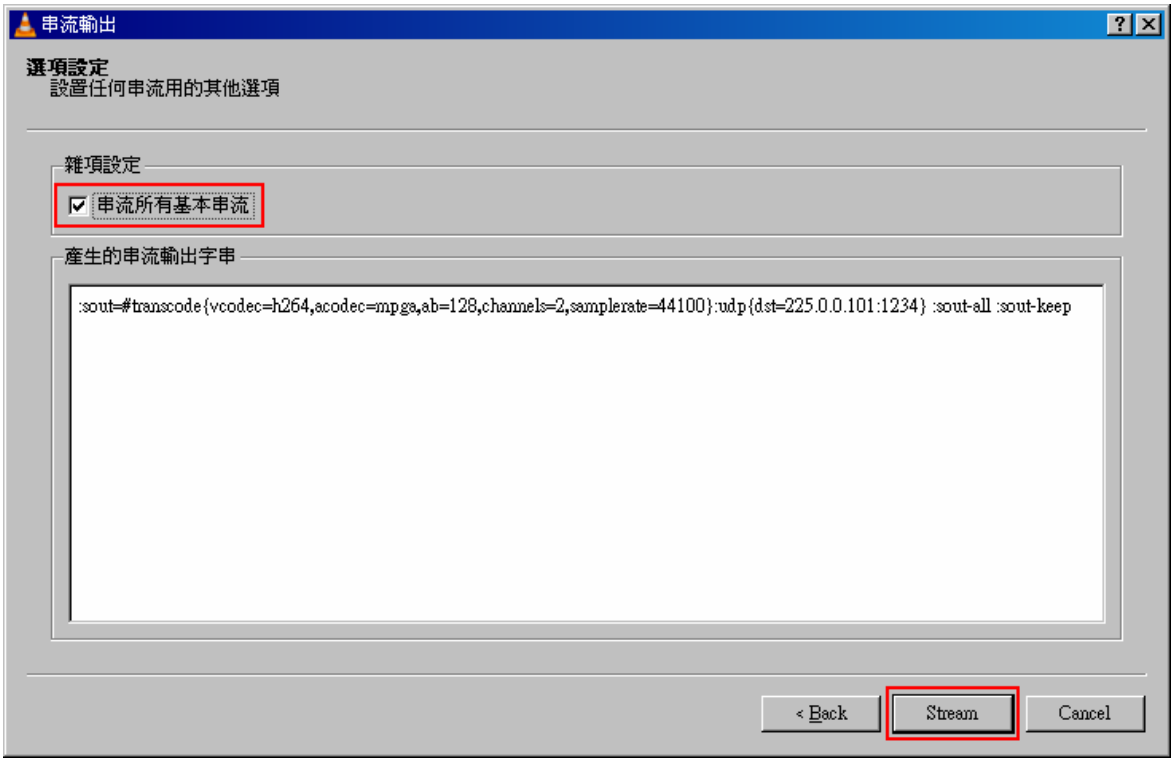


(5) Set stream IP, the range is 224.0.0.1 to 239.255.255.254, and protocol port is 1234.

Here I set stream IP is 255.0.0.1.

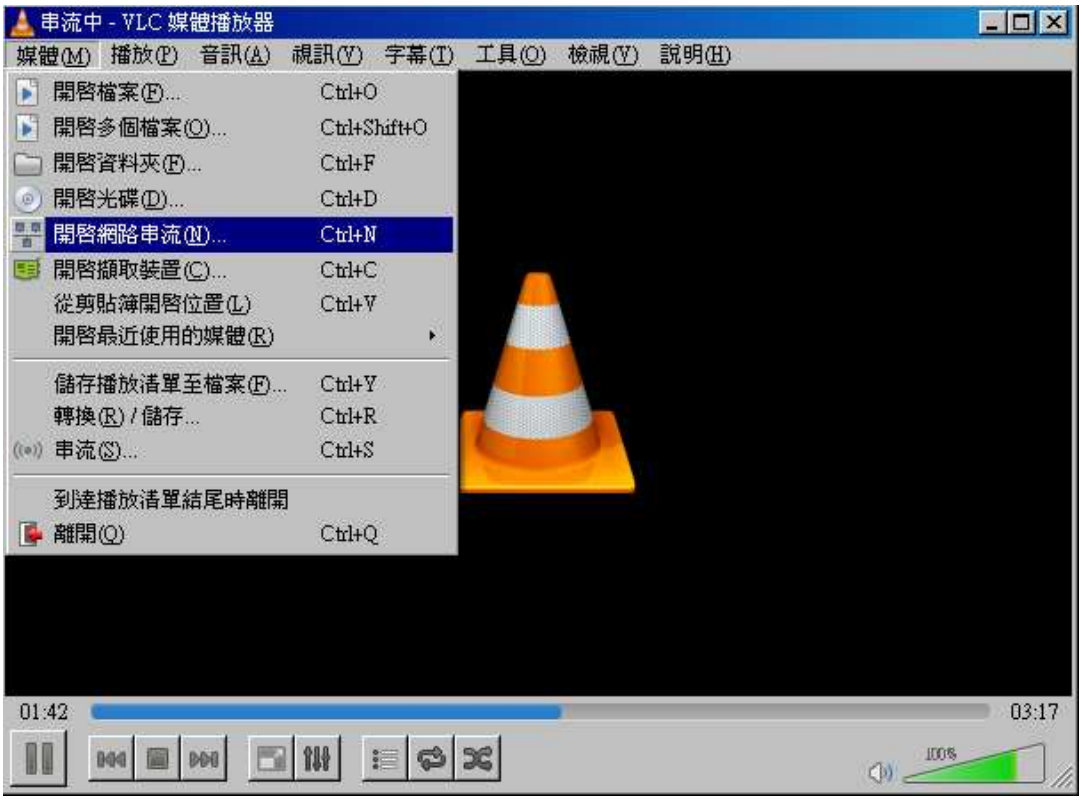


(6) Select ”Sort out all stream” and click “Stream” button, then the stream start to send to switch.



VLC Configure on IGMP Client

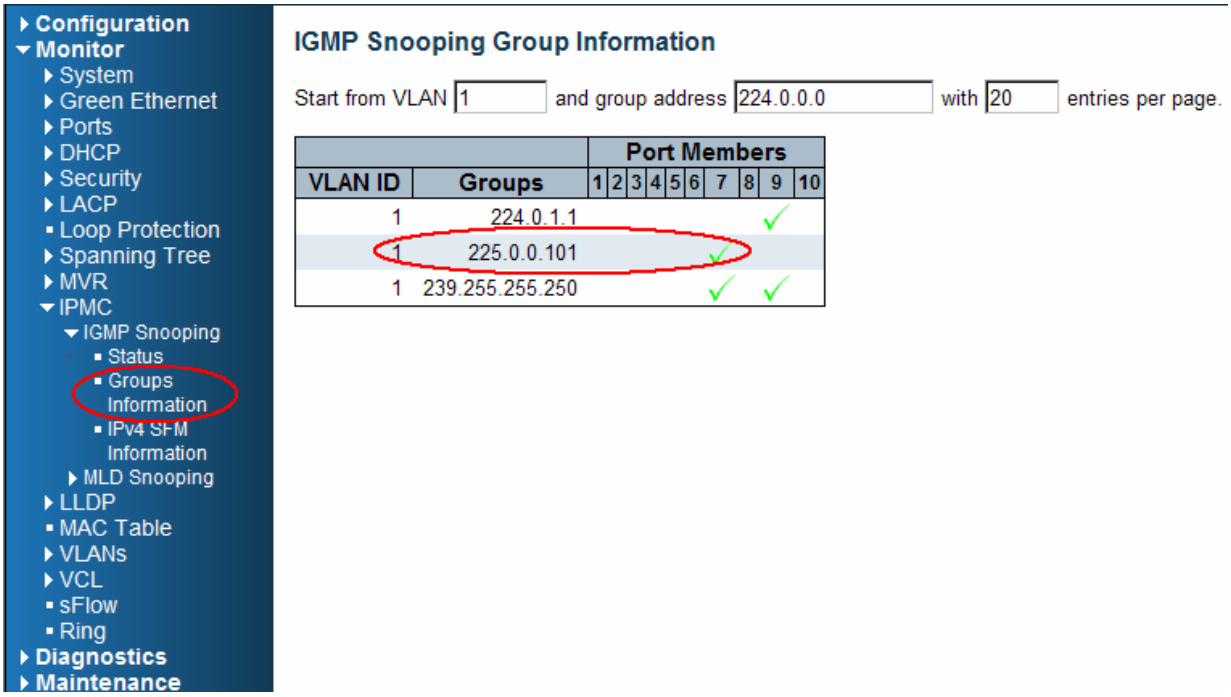
(1) In «Media » area of top tool bar to select open network stream



(2) Set the stream IP and protocol port as previous setting on server, the protocol type is “UDP”, the format should as below circle, then click “PLAY” button.

Back to management switch,

Go to “Monitor→ IPMC→ Groups Information”, you will see the stream IP in the table.



802.1x Authentication Application Guide

Introduction of 802.1x authentication function

IEEE 802.1x derives keys which can be used to provide per-packet authentication, integrity and confidentially. Typically use along with well-known key derivation algorithms (e.g. TLS, SRP, MD5-Challenge, etc.). In our industrial switch (FSM-510G), we support 802.1x authentication function per port (port1~port10). You should enable 802.1x function of the system, and choose ports and type you want to apply. If FSM-510G enable 802.1x authentication control for certain Ethernet port, this port should be authenticated before using any service from the network. Please see the following description.

802.1x Timer in FSM-510G

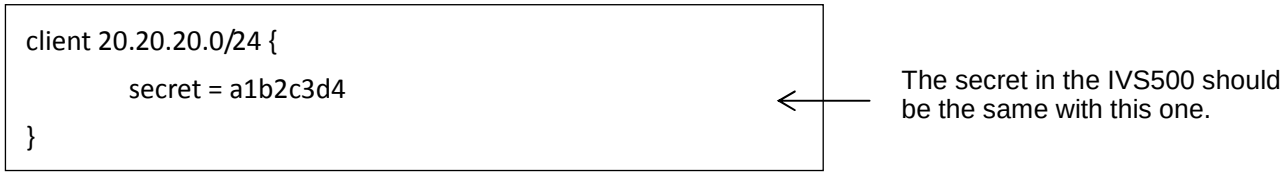
Item	Parameter (sec)	Description
1	ReAuth Period	FSM-510G will restart authentication after each Reauth-Period when authentication success and ReAuth option is enabled
2	Quiet Period	FSM-510G will wait QuietPeriod to restart authentication process again when authentication failed in previous time.
3	Tx Period	FSM-510G will send EAP-request to Supplicant every TxPeriod when authentication is running and Quiet Period is not running.
4	Supplicant Timeout	FSM-510G will wait SupplicantTmeout to receive response from Supplicant.
5	Server Timeout	FSM-510G will wait ServerTimeout to receive response from RADIUS server.

Configuration in RADIUS Server

Step 1: Prepare a Linux PC with RADIUS server installed.

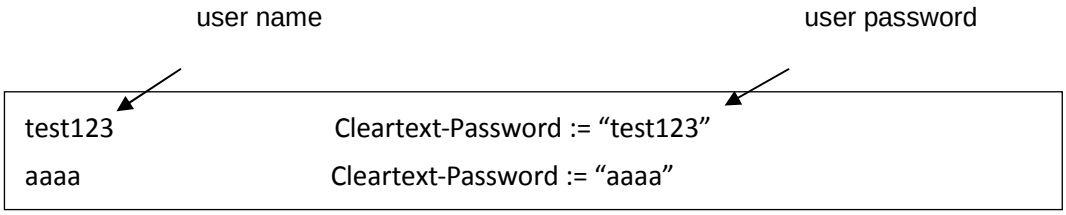
Step 2: Edit secret key for Radius server.

Setting:


client 20.20.20.0/24 {
secret = a1b2c3d4
}
The secret in the IVS500 should be the same with this one.

Step 3: Edit user name and password for supplicant to authenticate with server.

Setting:



Step 4: Set a static IP address for this Radius Server.

Setting: 20.20.20.20

Step 5: Start Radius Server

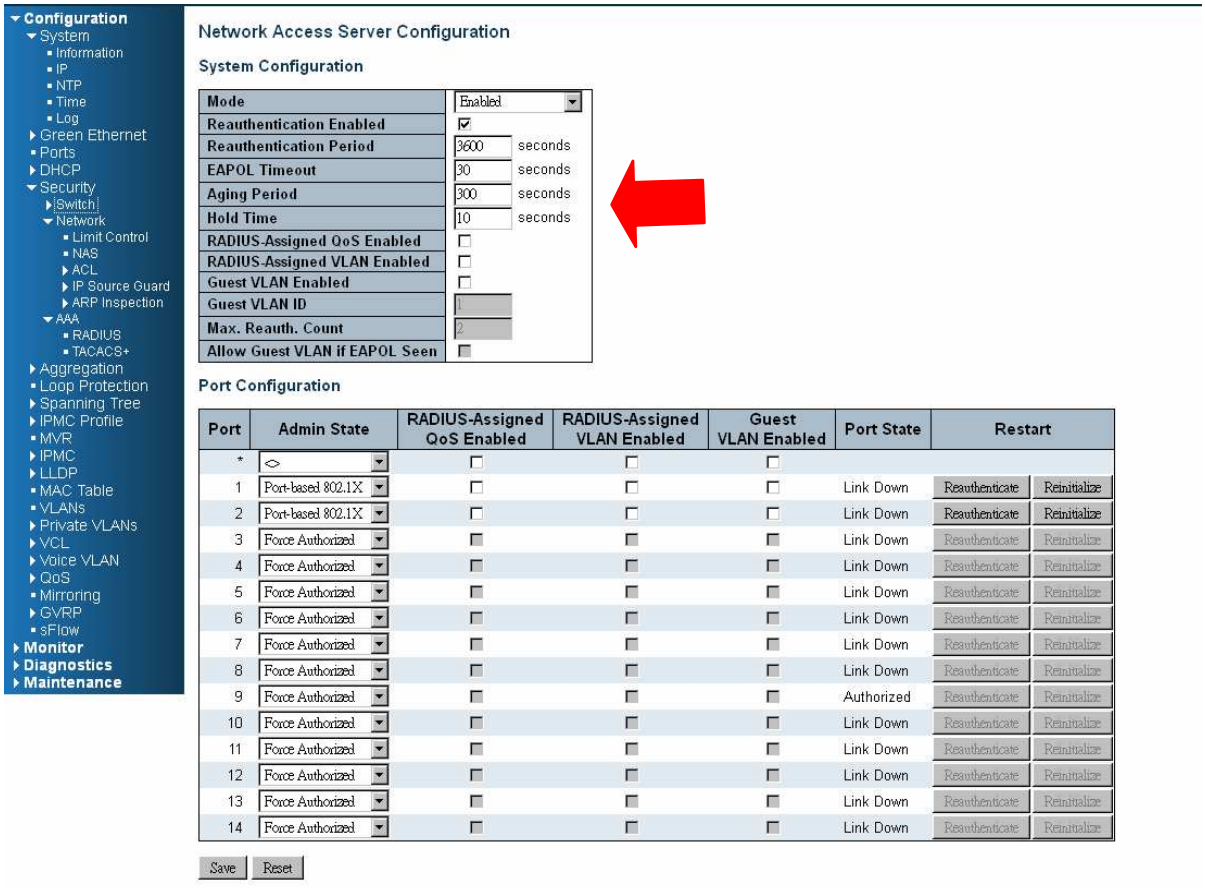
Example

Here we take an example of 802.1x Authentication via FSM-510G to be authenticated by RADIUS server. In a basic example, we take port 1 as a testing port which enables 802.1x in FSM-510G.

With default configuration, use the following Web UI setting .

Step1. Go to Configuration -> Security -> Networks -> NAS.

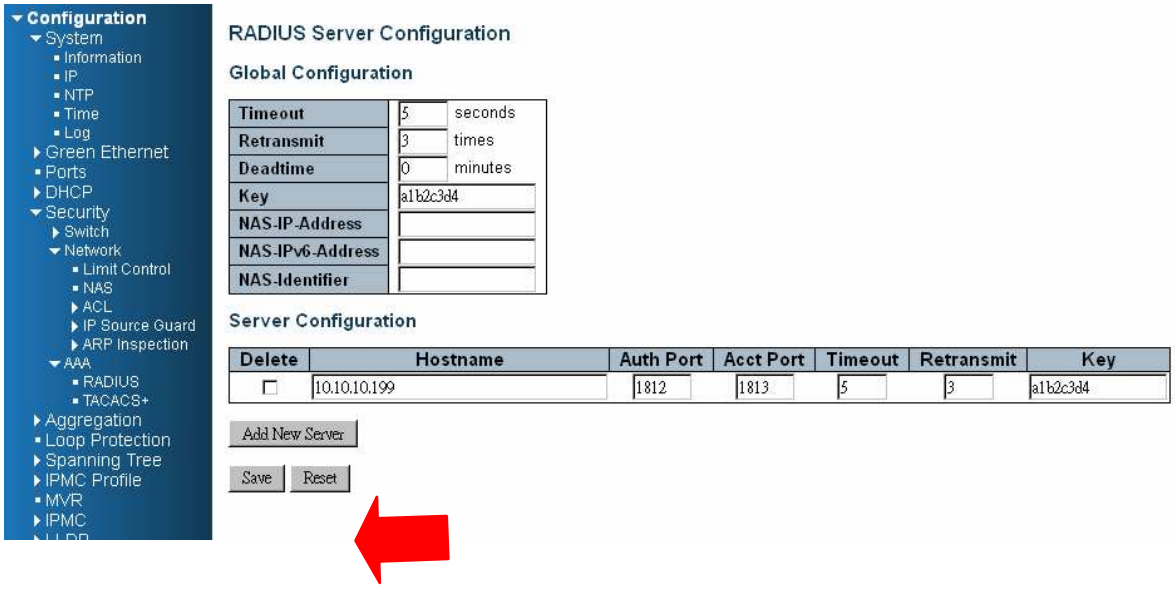
Select “Enable” mode to enable authentication, and set port-1, port-2 be “Port Base 802.1x”.



Step1. Go to Configuration -> Security -> AAA -> Radius.

Click “Add New Server”, Input “20.20.20.20” for server, and “a1b2c3d4” for secret key.

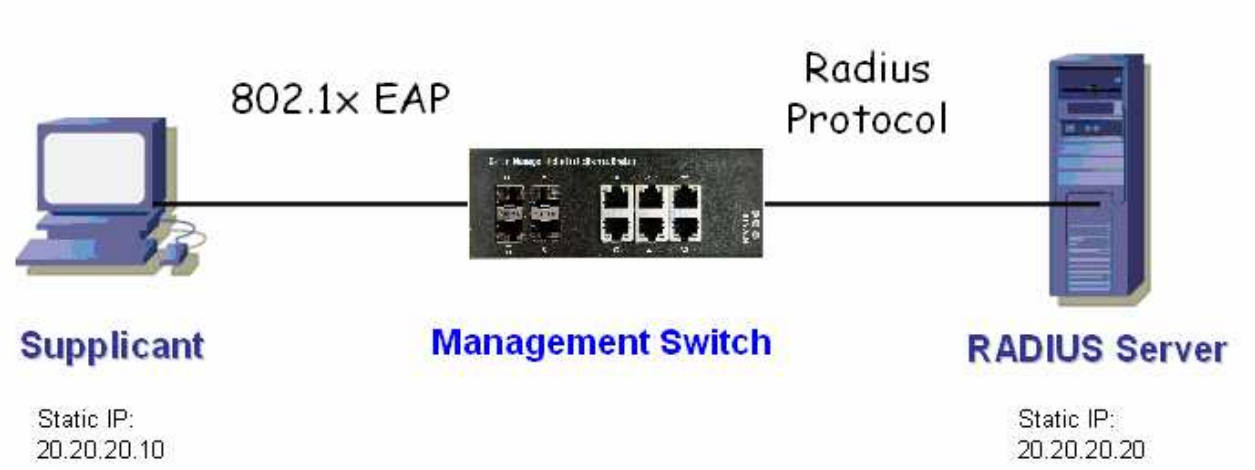
Then click “Save” button.



CLI Command:

```
configure
interface vlan 1
ip address 20.20.20.120 255.0.0.0exit
exit
radius-server host 20.20.20.20 timeout 5 retransmit 3 key a1b2c3d4
dot1x re-authentication
dot1x system-auth-control
exit
interface GigabitEthernet 1/1
dot1x auth-port-control auto
```

Configuration



Supplicant's NIC Setting

Step 1: Configure a static IP address 20.20.20.10 and net mask 255.255.255.0 for supplicant.

(If there is a DHCP server to assign IP address for supplicant, this step can be ignored.)

Step 2: Select the IEEE802.1x Authentication Enable check box, then to configure EAP type to MD5-Challenge.

After setting this function in NIC, supplicant should enter a correct pair of account and password in order to use this Ethernet port service from FSM-510G.

Authentication Behavior

Supplicant should pass authentication process in order to use any service. After supplicant enters correct account and password which stored in RADIUS server, it can be authenticated successfully. The authentication process is as following.