Industrial Managed Ethernet PoE Switch

User Guide

Version Number: 1.0
Issue: 1.2r1, July 2015

[CONTENTS]

[LIST OF TABLES]

[LIST OF FIGURES]

Preface

Preface

Scope

This document provides an overview on IPG500. It contains:

- Descriptive material about the IPG500 Hardware Installation Guide.

Audience

The guide is intended for system engineers or operating personnel who want to have a basic understanding of IPG500.

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*.

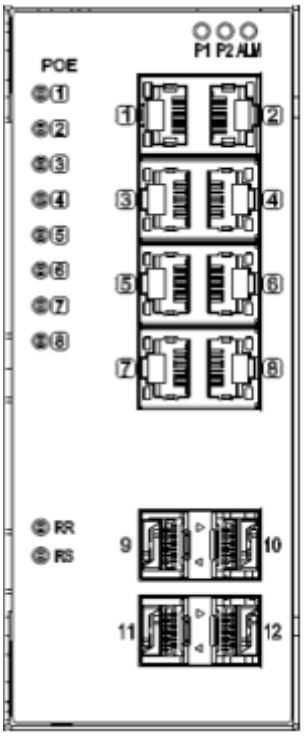
Note — The information supplements the text or highlights important points.

Overview

Overview

IPG500 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

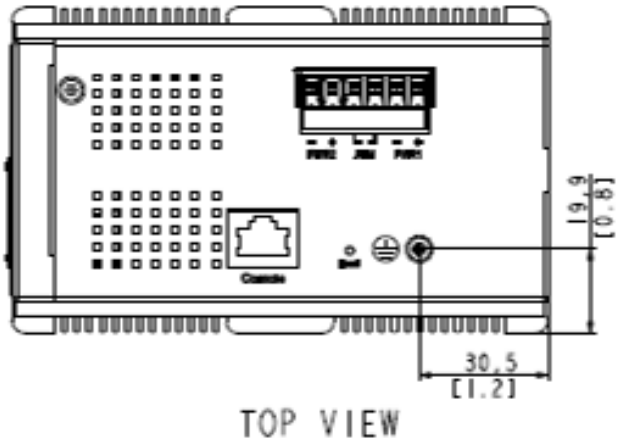


Front Panel Introduction

Front Panel	
System Status LED	P1, P2 and Alarm
Gigabit Ethernet Copper Ports	RJ45
Gigabit Ethernet SFP ports	SFP Slots
POE LED	POE port status
RR/RS LED	Device info/status

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
Power	
Power input	Redundant Input Terminals
Input voltage range	46~58 VDC
Max. power consumption	without PoE: 14W, With PoE: 265 W
Reverse power protection	Yes
Total PoE output power budget	240W
PoE PSE port output power management	Scheduling; power control; PoE PD power consumption monitoring
Transient protection	> 15,000 watts peak

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(H) x 128mm(D) x 77mm(W)
Weight	1410g

System statistics

Function Name	System Max Value
VLAN ID	4096
VLAN Limitation	1024
Privilege Level of User	15
RMON Statistic Entry	65535
RMON Alarm Entry	65
RMON Event Entry	65535
IPMC Profile	64
IPMC Rule / Address Entry	128
ACE	256
ICMP Type / Code	255
RADIUS Server	5
TACACS+ Server	5
MAC-based VLAN Entry	256
IP subnet-based VLAN Entry	128
Protocol-based VLAN Group	125
Voice VLAN OUI	16
QCE	256
IP Interface	8
IP Route	32
Security Access Management	16
MVR VLAN	4
MAC Learning table address	8k
IGMP Group	256

Quick Installation

Equipment Mounting

Cable Connecting

Equipment Configuration

Quick Installation

Mounting the IPG500 (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.

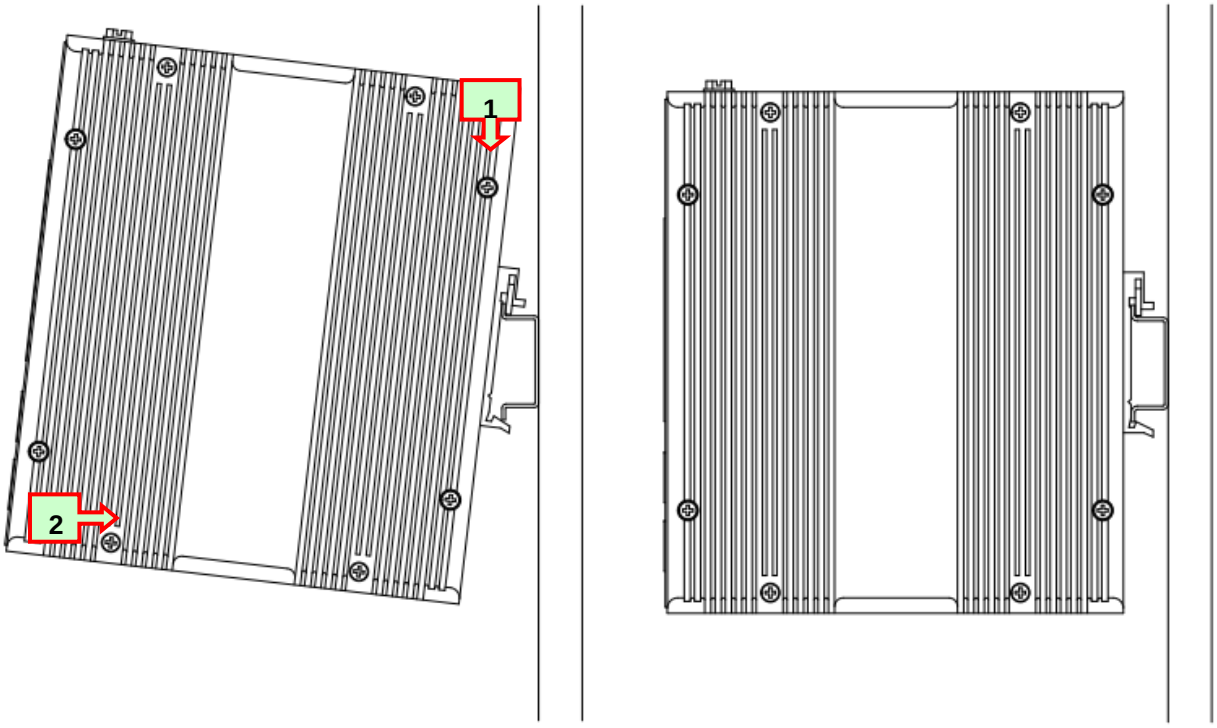


Figure 1 DIN-Rail Mounting

Mounting the IPG500 (Wall mount)

Mounting step:

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

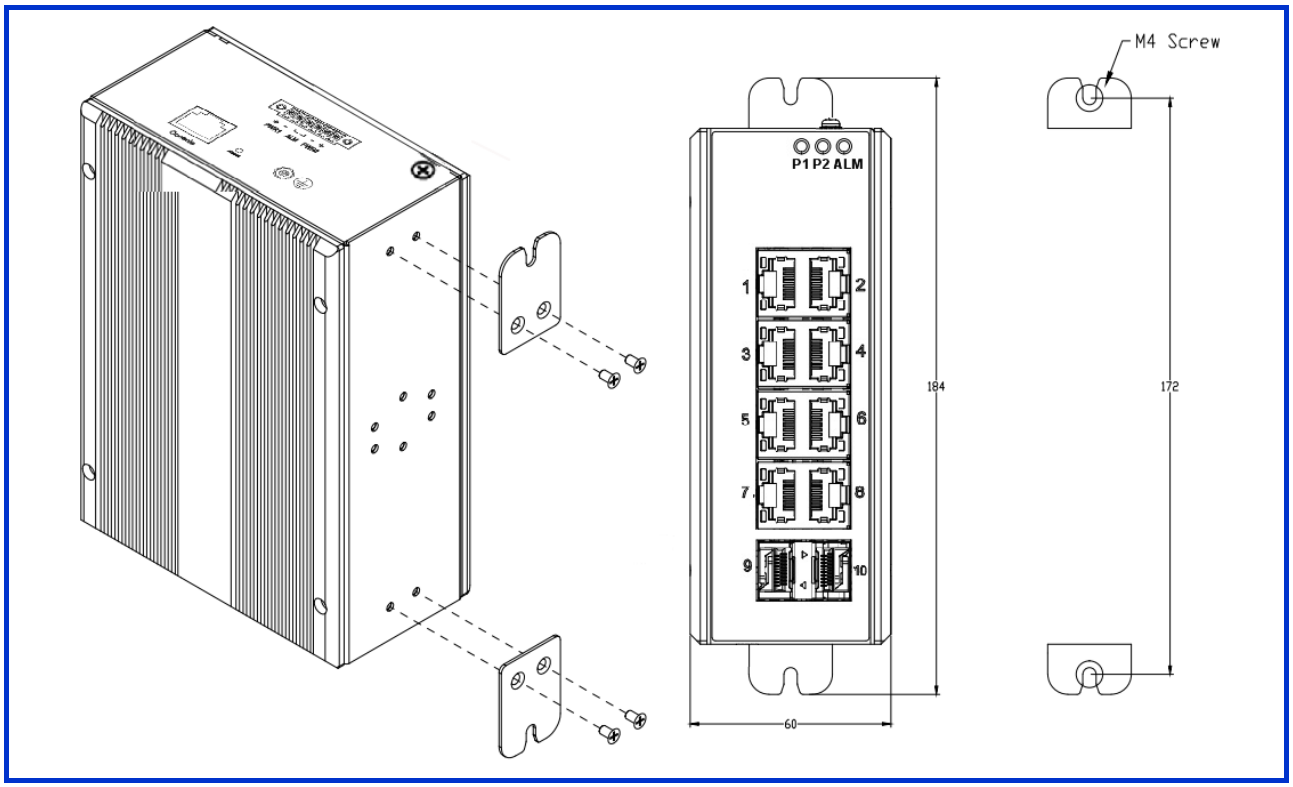
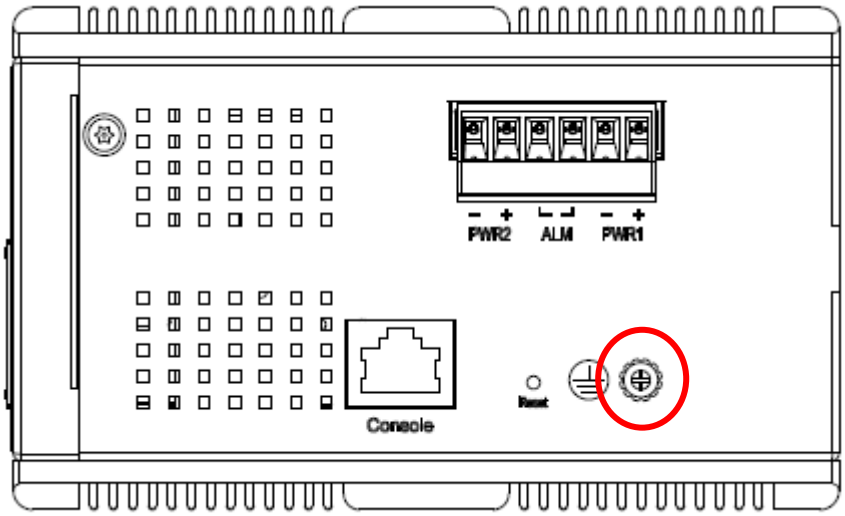


Figure 2 Wall Mounting

Ground Connections

IPG500 must be properly grounded for optimum system performance.

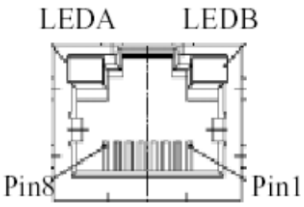


Connecting the Ethernet Interface (RJ45 Ethernet)

IPG500 provides two types of electrical (RJ45) and optical (mini-GBIC) interfaces.

- To connect to a PC, use a straight-through or a cross-over Ethernet cable,
- To connect the IPG500 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.

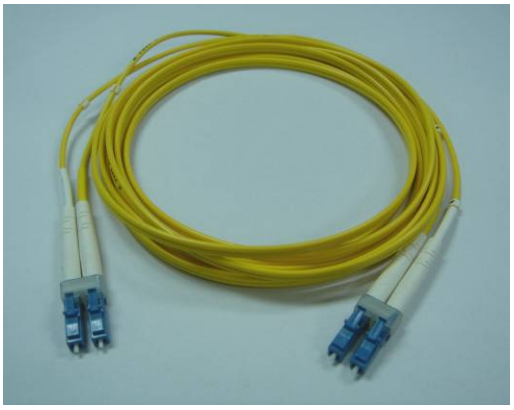


Pin	Assignment	PoE Assignment
1,2	T/Rx+,T/Rx-	Positive V_{Port}
3,6	T/Rx+,T/Rx-	Negative V_{Port}
4,5	T/Rx+,T/Rx-	X
7,8	T/Rx+,T/Rx-	X

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.

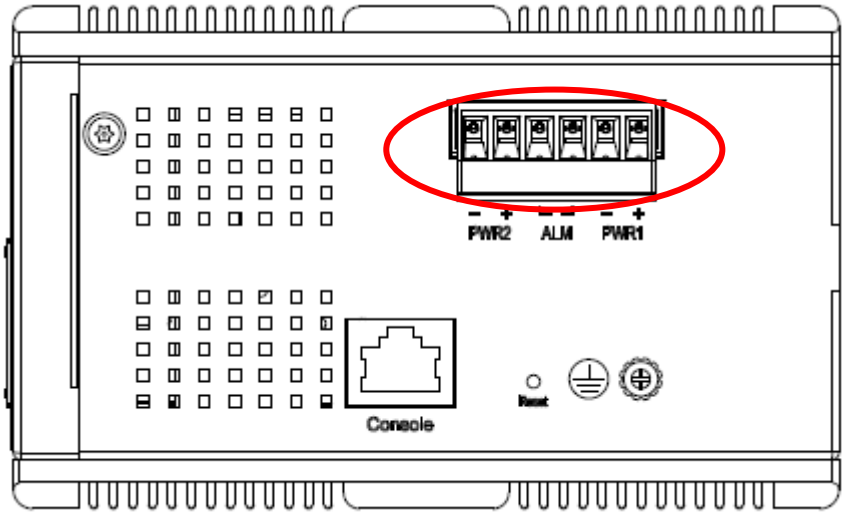
Do not power up the laser product without connecting the laser to the optical fiber and putting the cover in position, as laser outputs will emit infrared laser light at this point.

Power Connection

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

The IPG500 can be powered from two power supply (input range 46V –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.



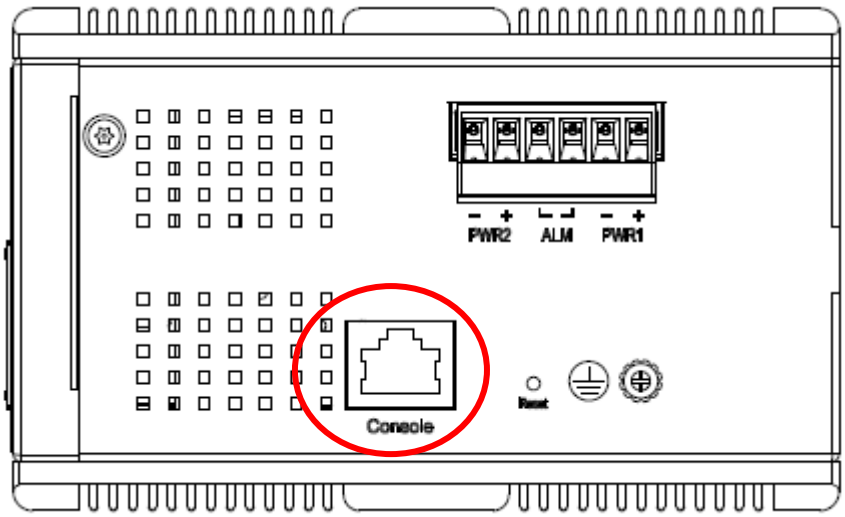
Power Connector (6P Terminal Block)	
Input	DC 46-58V
PWR1 +/-	Power Input 1 +/-
PWR2 +/-	Power Input 2 +/-
ALM	Alarm relay output

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

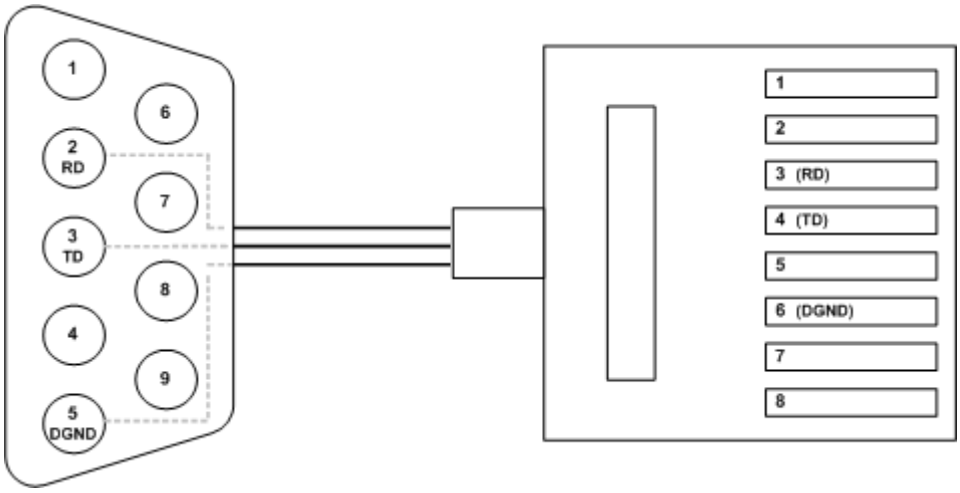
Console Connection

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

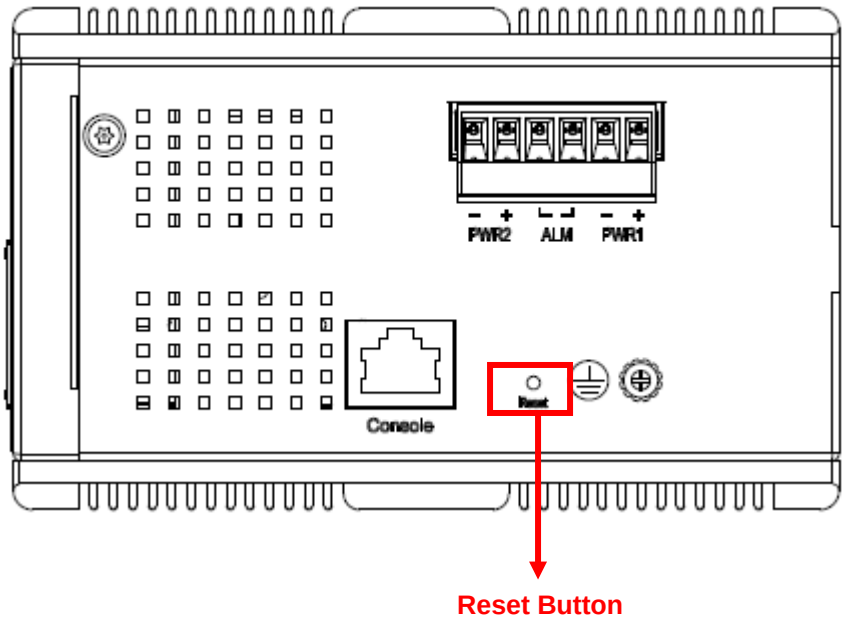


To connect the host PC to the Console port, a RJ45 (male) connector-to-RS232 DB9 (female) connector cable is required. The RJ45 connector of the cable is connected to the Console port of IPG500; the DB9 connector of the cable is connected to the PC COM port. The pin assignment of the Console cable is 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 IPG500 may not respond; then you may need to push the 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 IPG500

1. Connecting to IPG500 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)

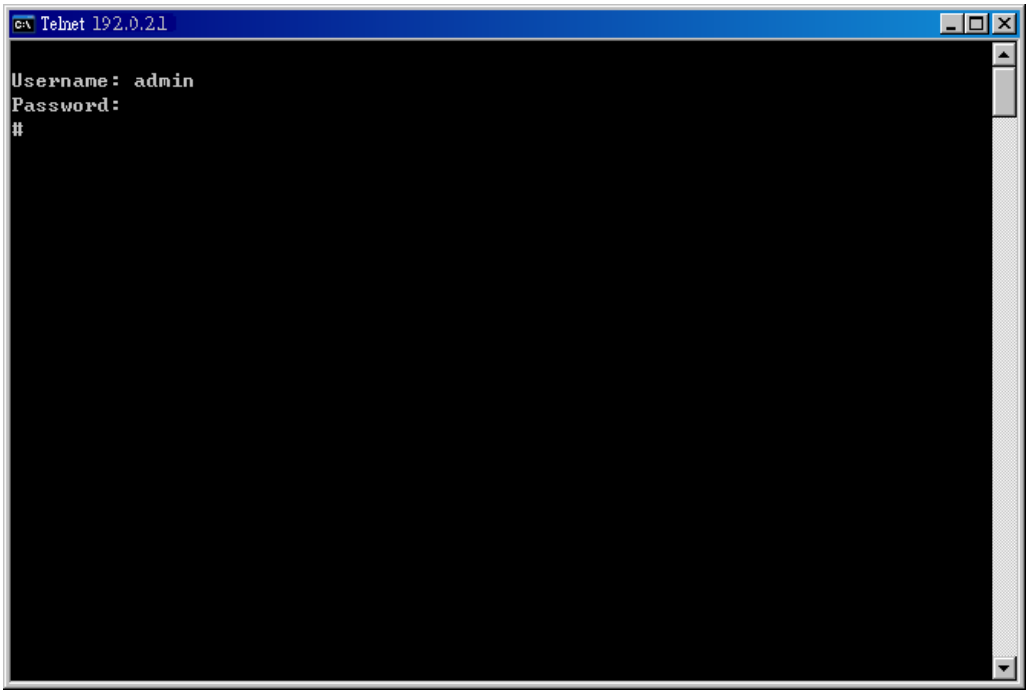
1. Connecting to IPG500 Ethernet port(RJ45 Ethernet port)

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:

   CLI Command:

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

Monitoring the Ethernet Interface

By RJ45 Ethernet:

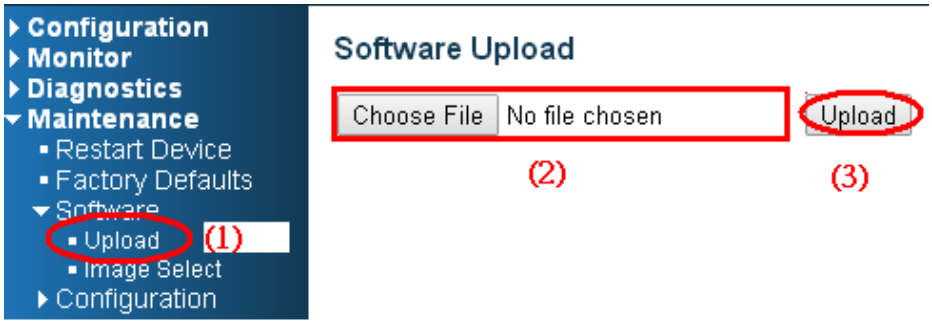
Refer to Figure 3 for monitoring 8 Gigabit Ethernet with copper connector (RJ45). Also refer to Table 1 for the normal operational LED status.

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

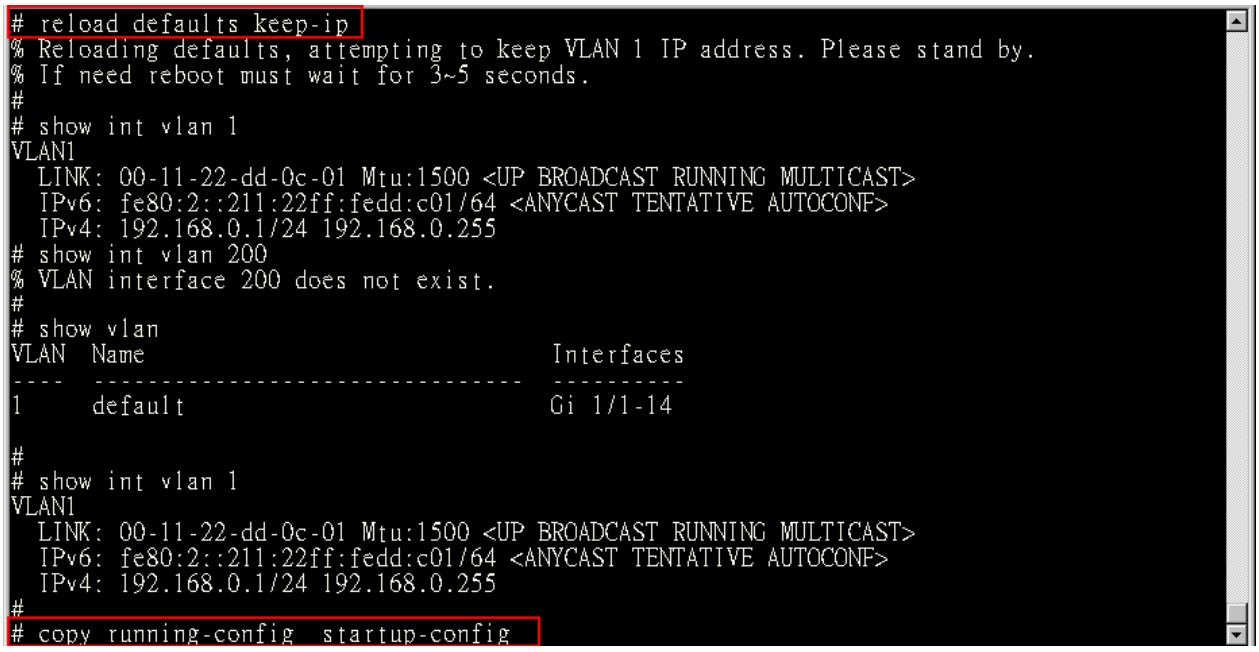
To see what current interface and IP address is:

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

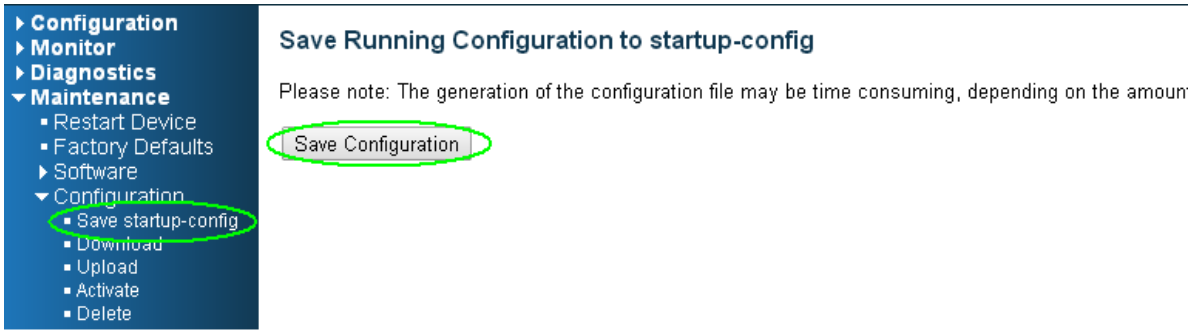
```
# reload defaults
% Reloading defaults. Please stand by.
% If need reboot must wait for 3~5 seconds.
# show int vlan 1
VLAN1
  LINK: 00-11-22-dd-0c-01 Mtu:1500 <UP BROADCAST RUNNING MULTICAST>
  IPv4: 192.0.2.1/24 192.0.2.255
  IPv6: fe80:2::211:22ff:fedd:c01/64 <ANYCAST TENTATIVE AUTOCONF>
# show vlan
VLAN  Name                             Interfaces
----  -------------------------------  ----------
1     default                          Gi 1/1-14

# copy running-config  startup-config
Building configuration...
% Saving 1357 bytes to flash:startup-config
% If need reboot must wait for 3~5 seconds.
#
```

Configuration via WEB UI

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

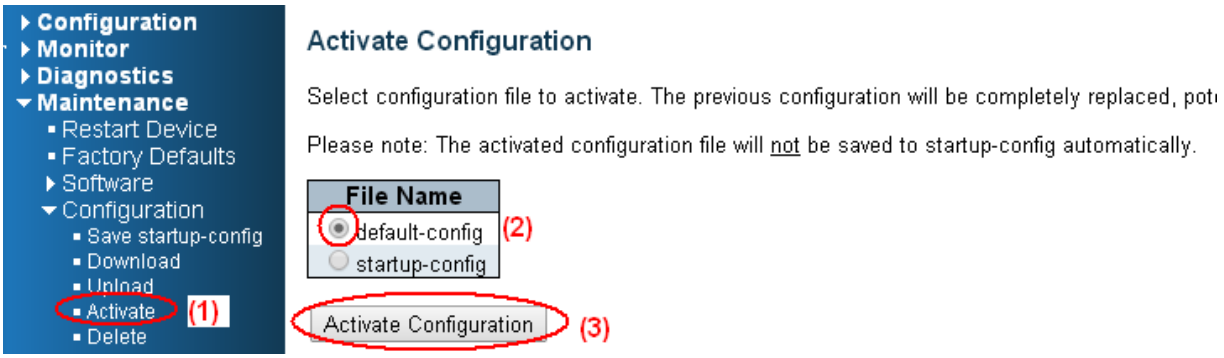
(1)Go to “Maintenance”→”Factory Defaults” pagination to Click “Yes” button.

(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

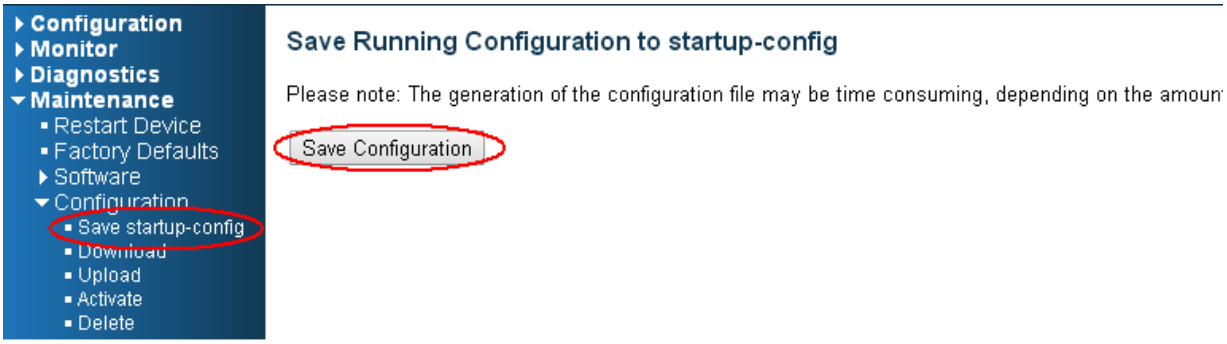
(1) Go to “Maintenance”→ “Configuration”→”Activate” pagination to select “default-config”, then click “Activate Configuration” button



(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 DUT'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
PoE	On Green	POE is detected
	Off	No link

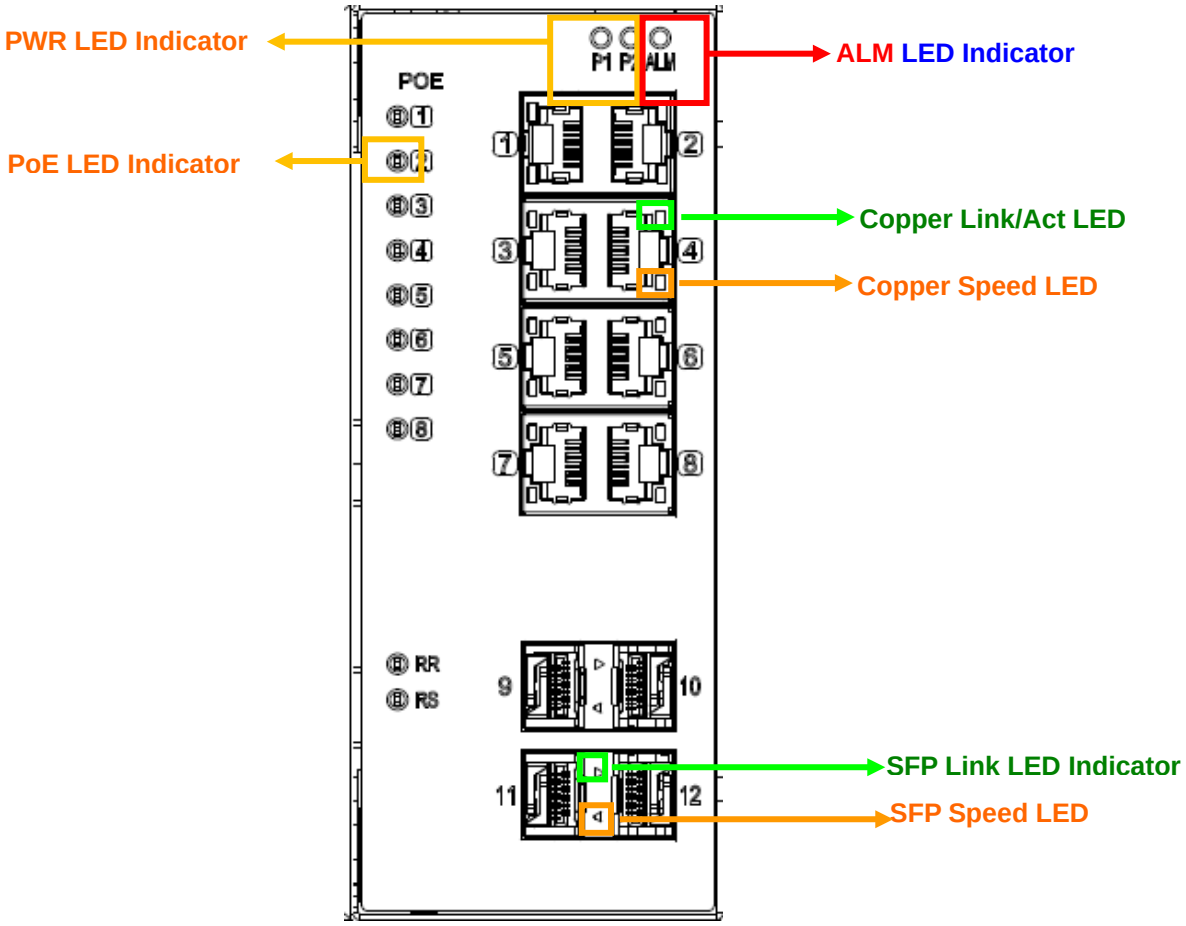


Figure 3 LED Indicators

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

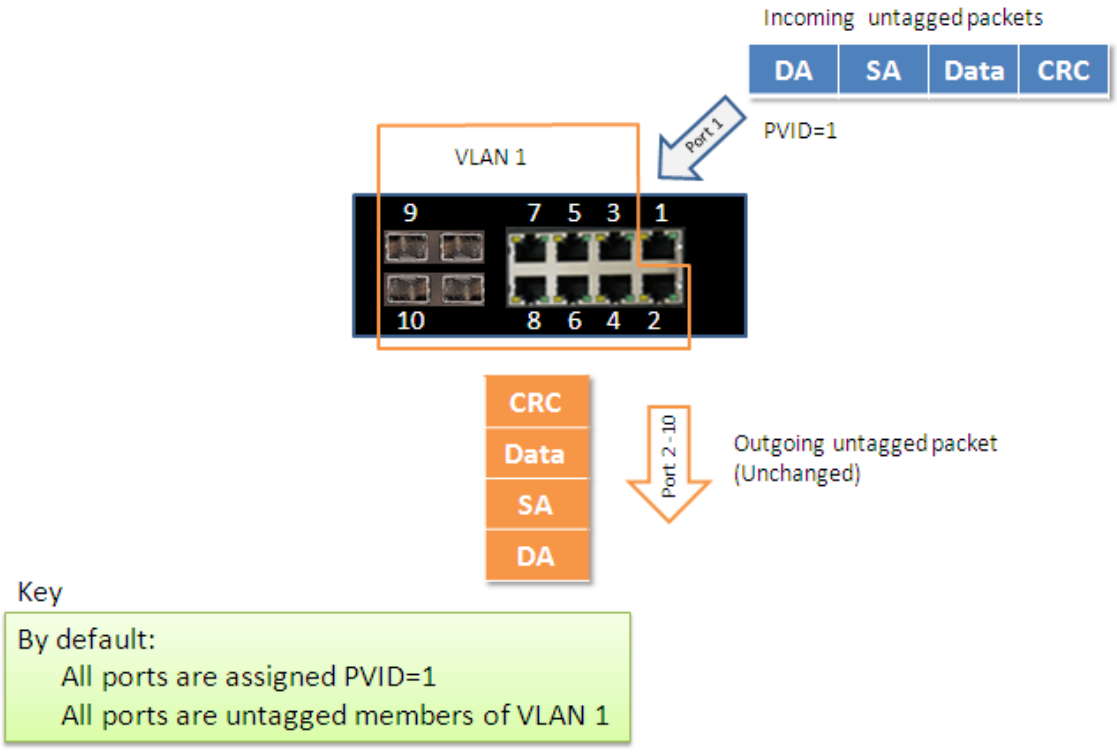
VLAN Application Guide

This part describes how to configure Virtual LANs (VLANs) in IPG500. The IPG500 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

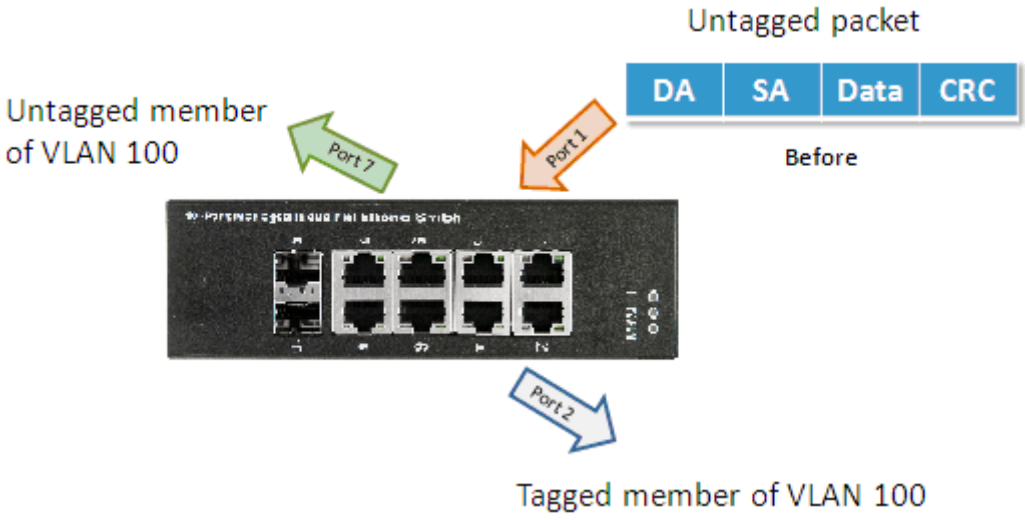
Each port in the IPG500 has a configurable default VLAN number, known as its PVID. This places all ports on the same VLAN initially, although each port PVID is configurable to any VLAN number between 1 and 4094.

The default configuration settings for IPG500 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).



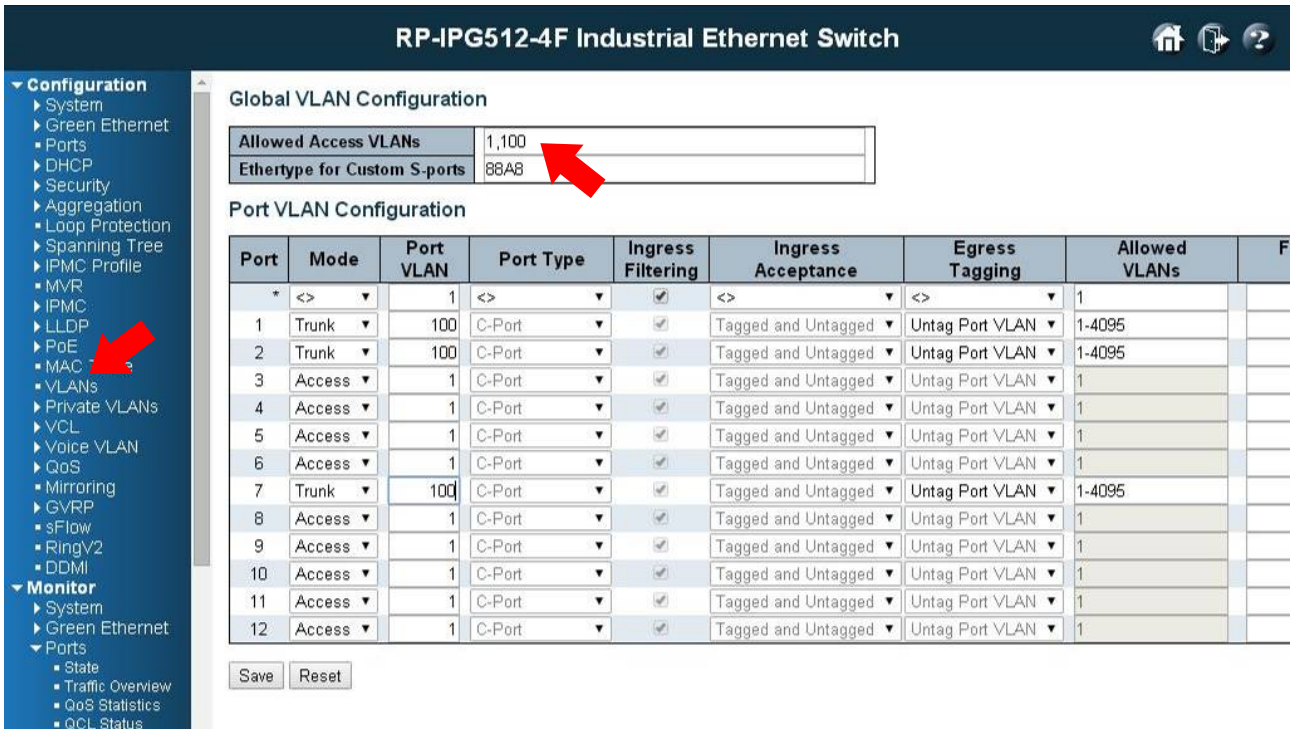
Example 2: Port-based VLANs

When the IPG500 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 IPG500 through Port 2, which is configured as a tagged member of VLAN100. The untagged packet remains unchanged as it leaves the IPG500 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.

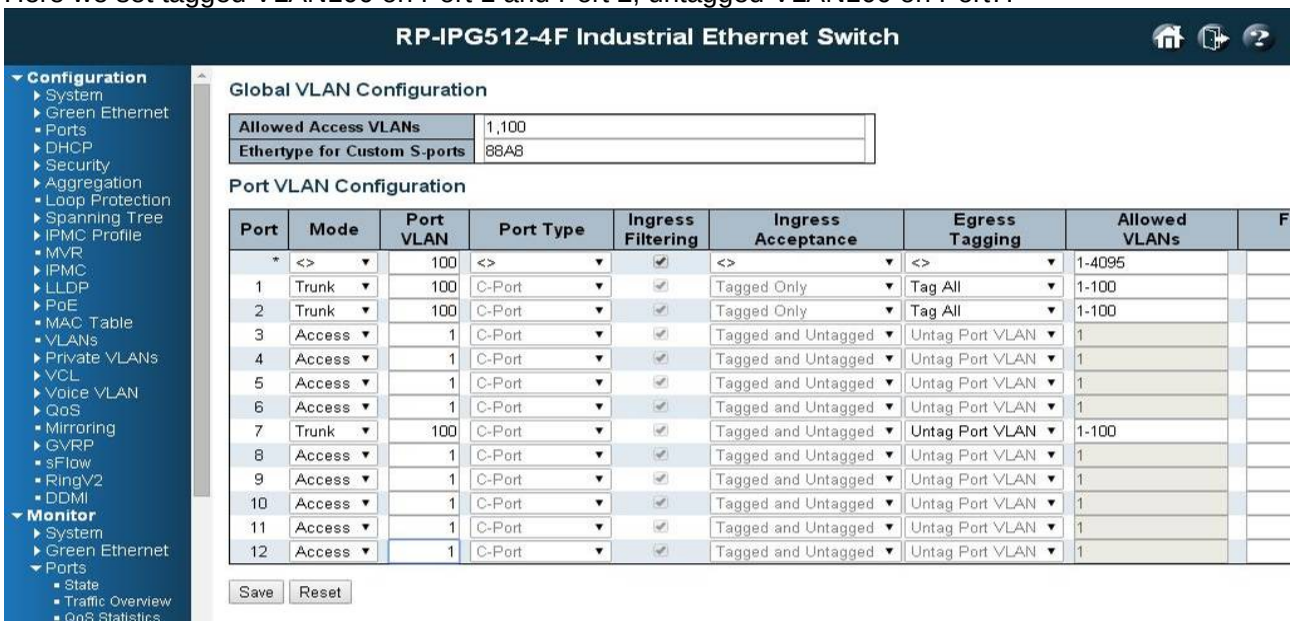


Step2. Select Configuration -> VLAN -> Static VLAN. Create a VLAN with VLAN ID 100. Enter a VLAN name in the **Name** field.

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 IPG500 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 IPG500 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 IPG500 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.

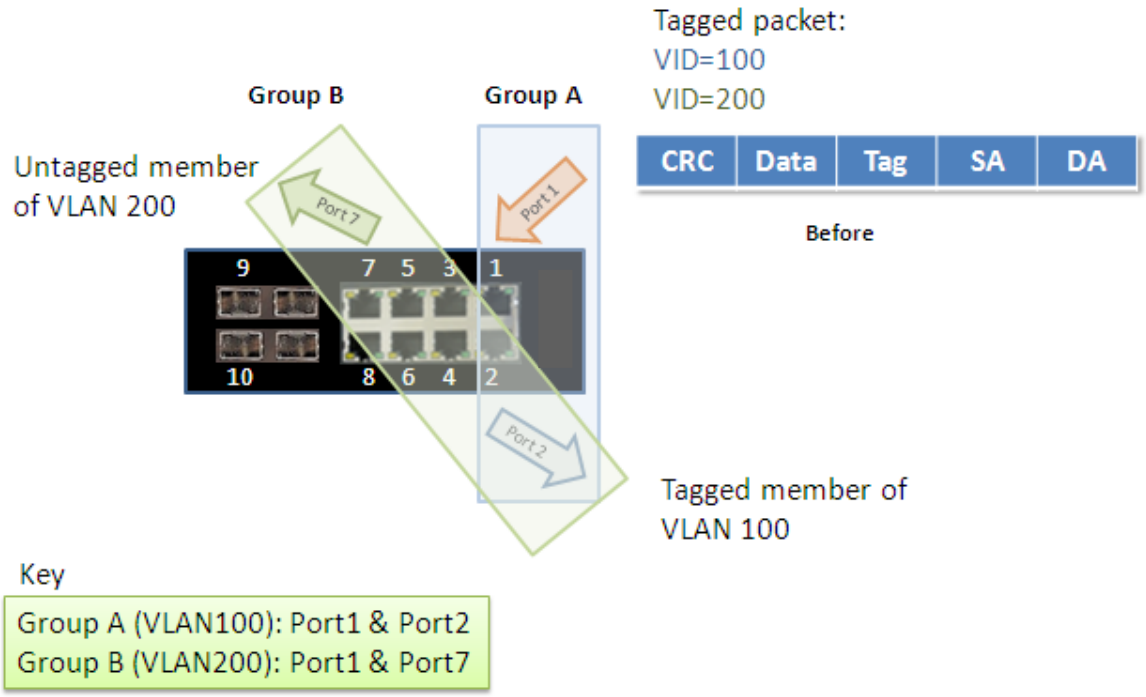
CLI Command:

```
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

IPG500 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.

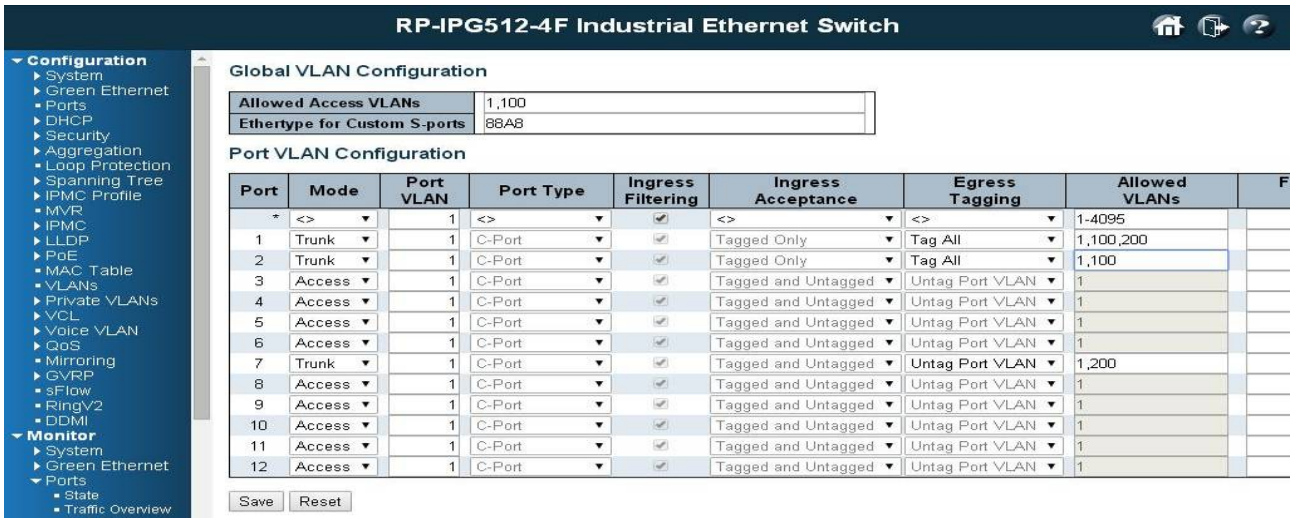
In the following figure, the tagged incoming packets are assigned directly to VLAN 100 and VLAN 200 because of the tag assignment in the packet. Port 2 is configured as a tagged member of VLAN 100, and Port 7 is configured as an untagged member of VLAN 200. Hosts in the same VLAN communicate with each 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 IPG500.

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 IPG500 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 IPG500 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 IPG500 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 IPG500 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.

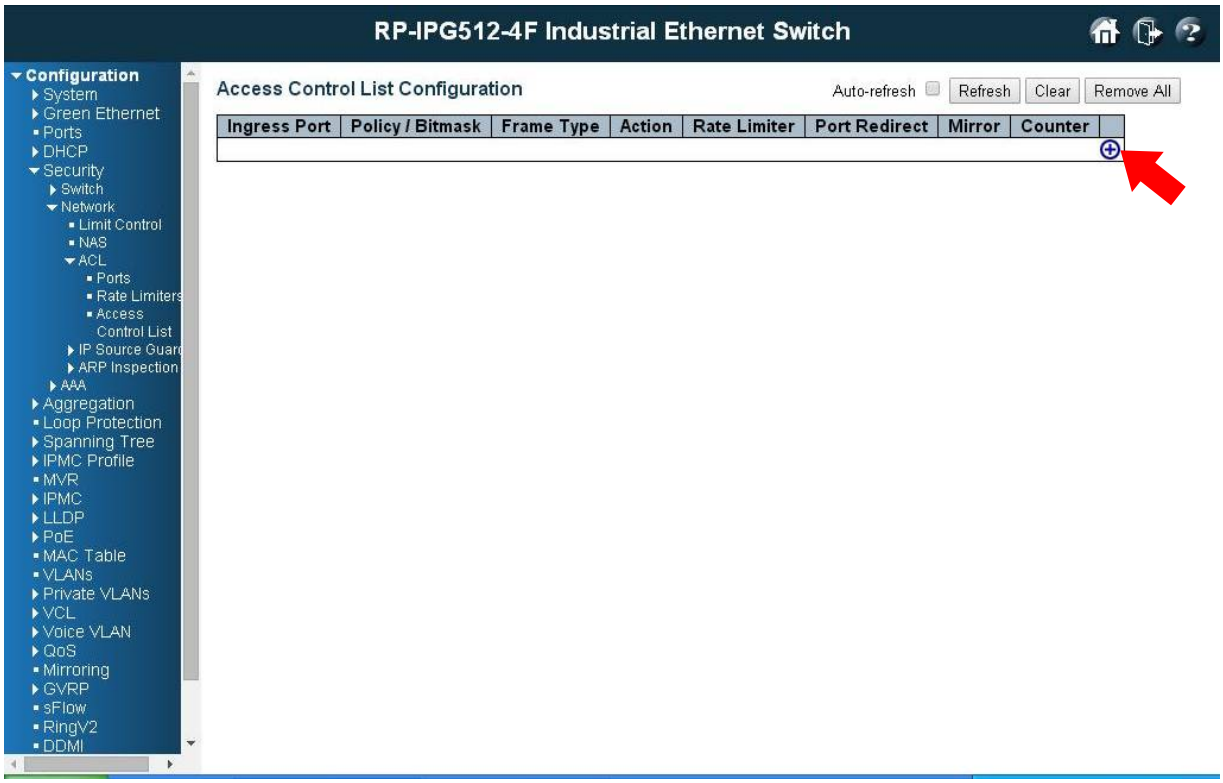
If user want to filter only one directional MAC address, the other MAC address just set to all zero. It means don't care portion. Besides MAC address, it also supports VLAN and Ether type for filter additionally. Certain VLAN or Ether type under these MAC address will take effect. If user doesn't care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

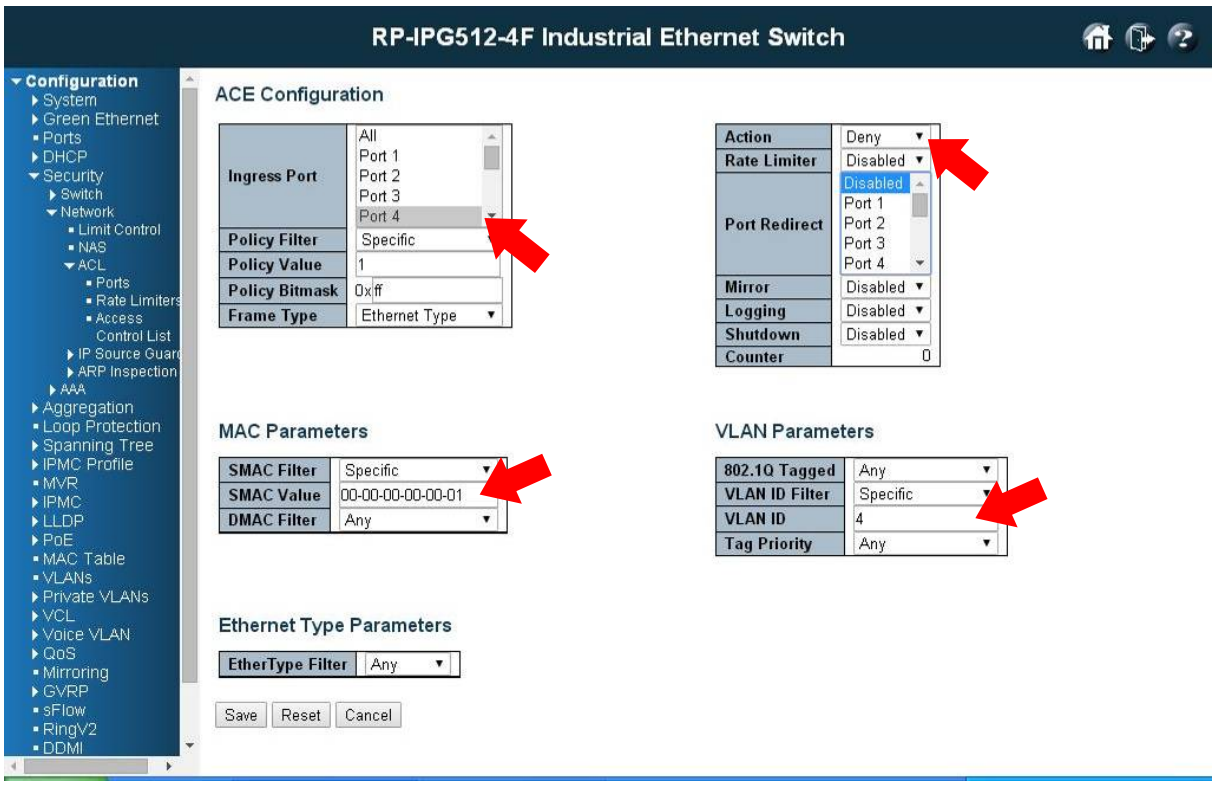
◎ One directional MAC address with one VLAN deny filtering.

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

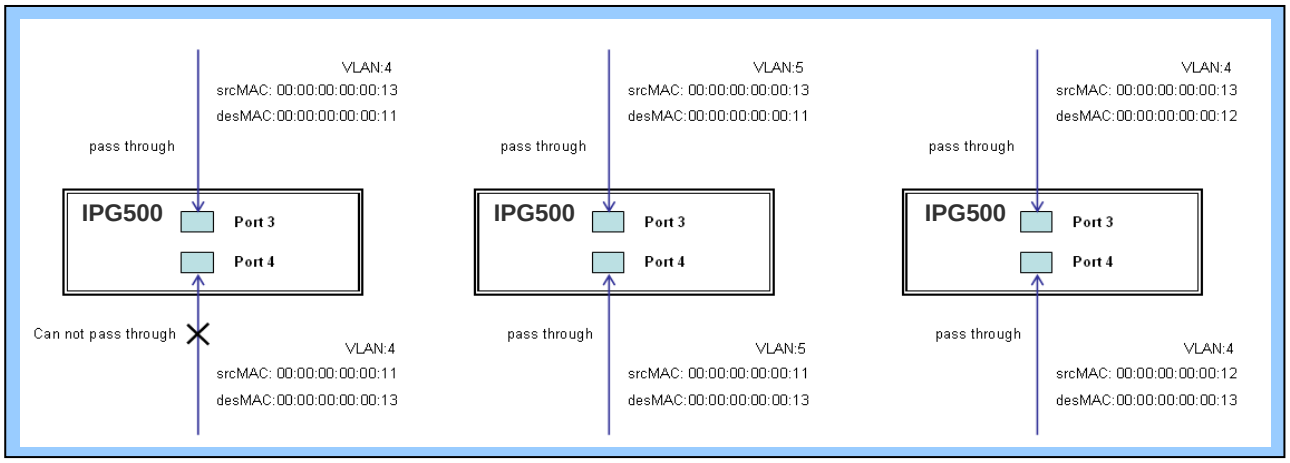


Step 2: Create a new ACL Entry rule under this ACL profile. (Deny MAC: 11 and VLAN: 4)

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:

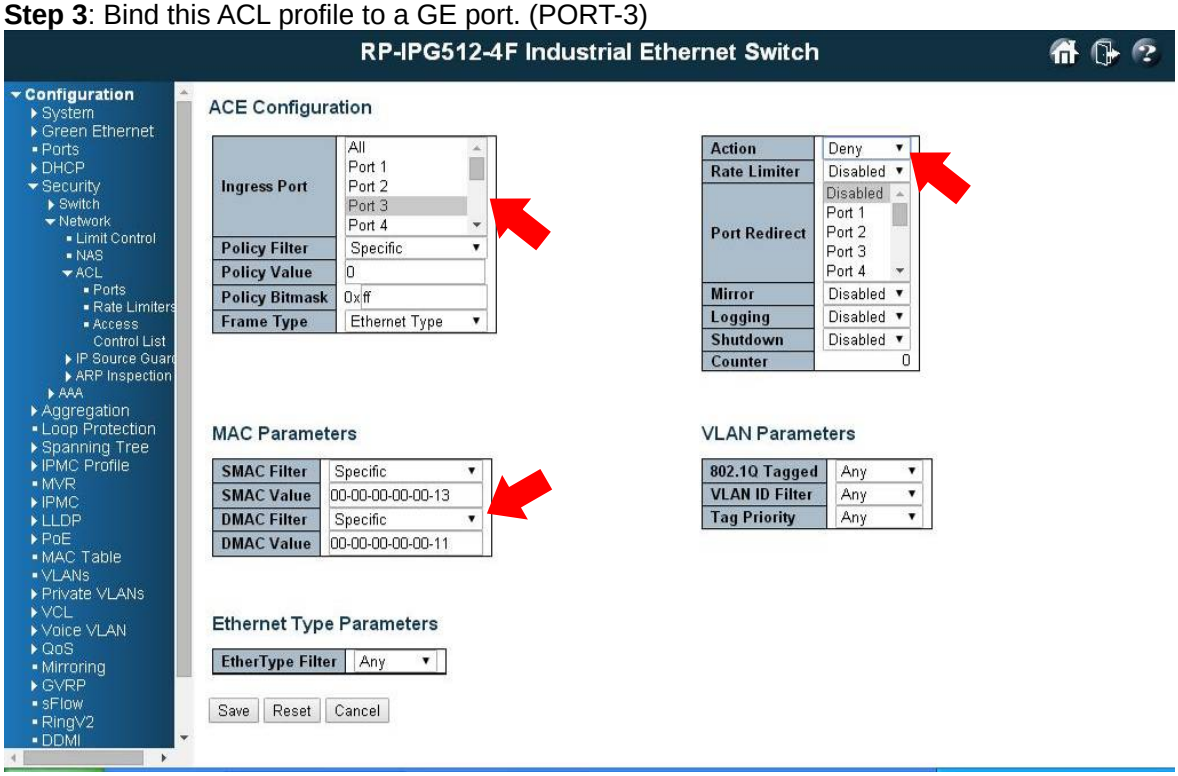
```
access-list ace 1 ingress interface GigabitEthernet 1/4 policy 1 vid 4
frametype etype smac 00-00-00-00-00-11 action deny
exit
interface GigabitEthernet 1/3
  switchport trunk allowed vlan 4,5
  switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
  switchport trunk allowed vlan 4,5
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

◎ Two directional MAC address with all VLAN deny filtering.

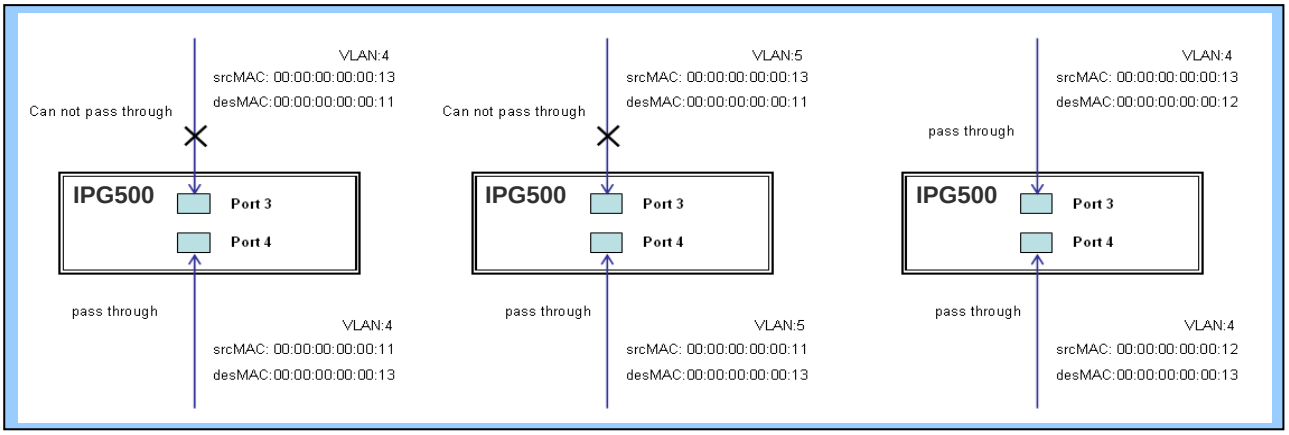
Step 1: Create a new ACL Profile. (Profile Name: DenySomeMac)

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.

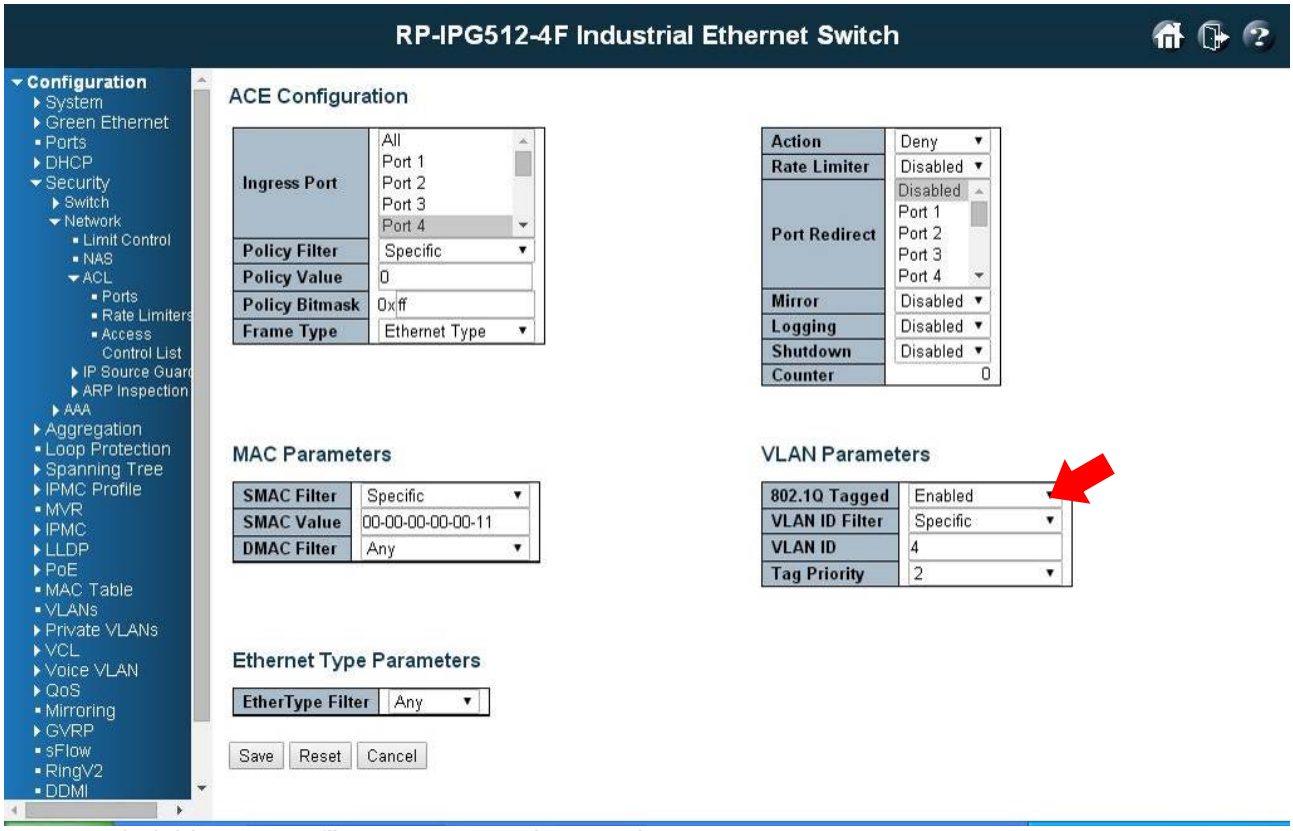
- **Case 1: (d)**

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)

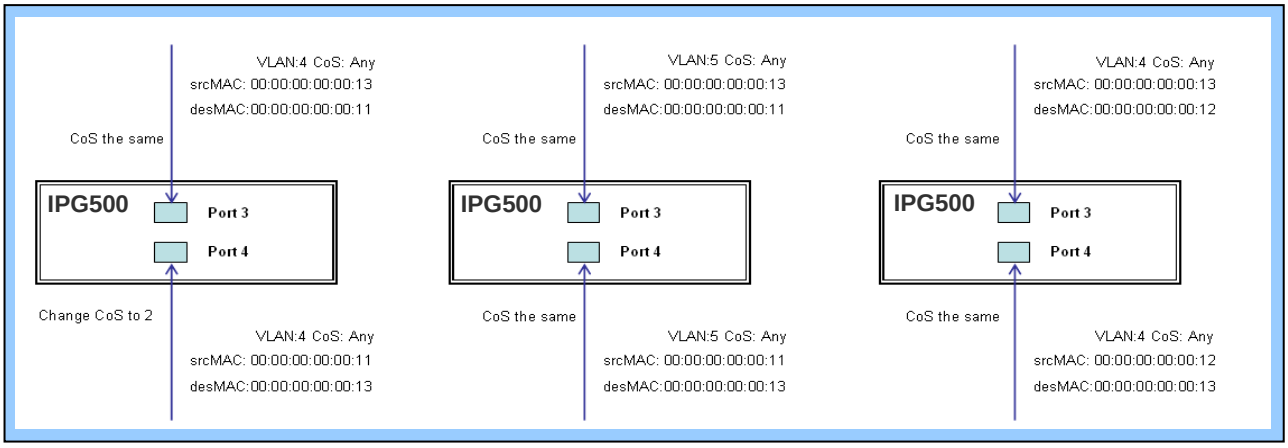
Step 1: Create a new ACL Profile. (Profile Name: CoSMarkingTest)

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.

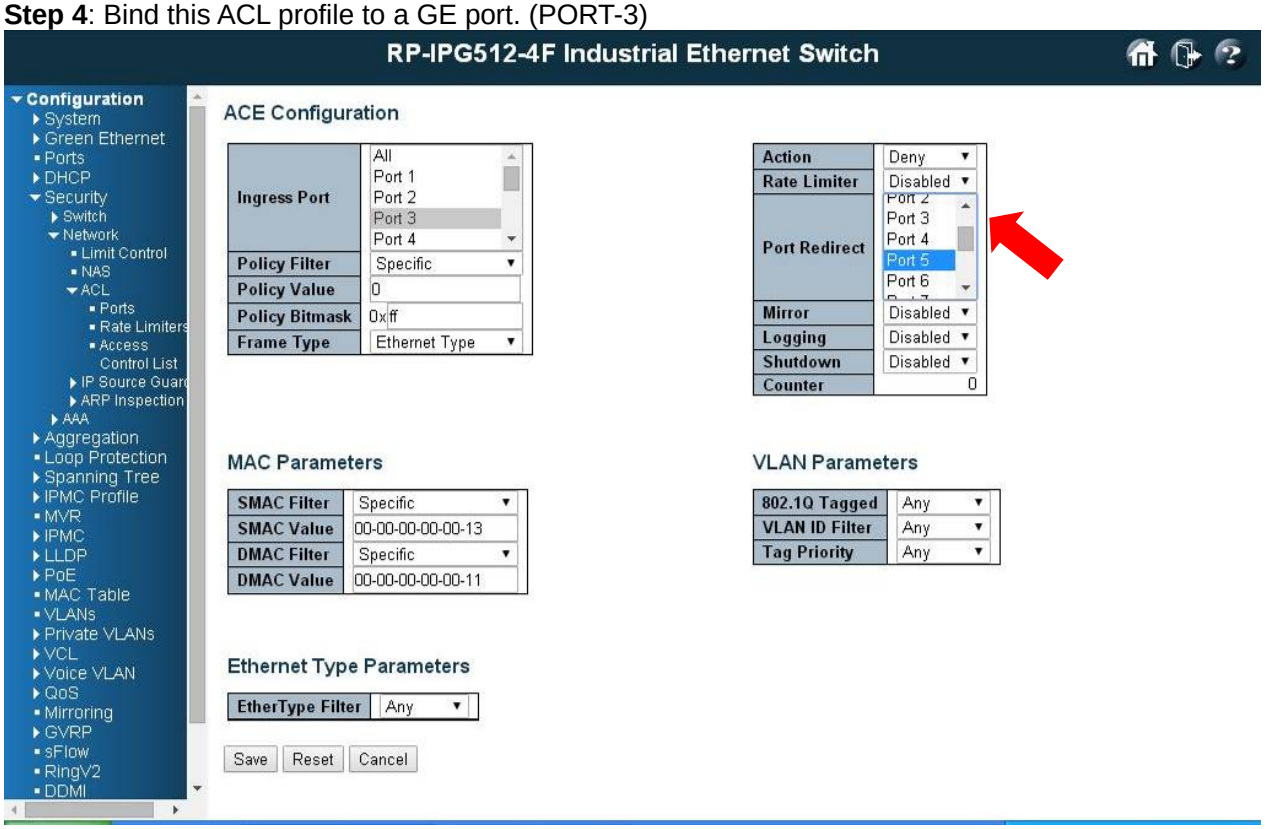
◎ Two directional MAC address with Copy Frame action.
(Don’t care VLAN ID, Ether Type)

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

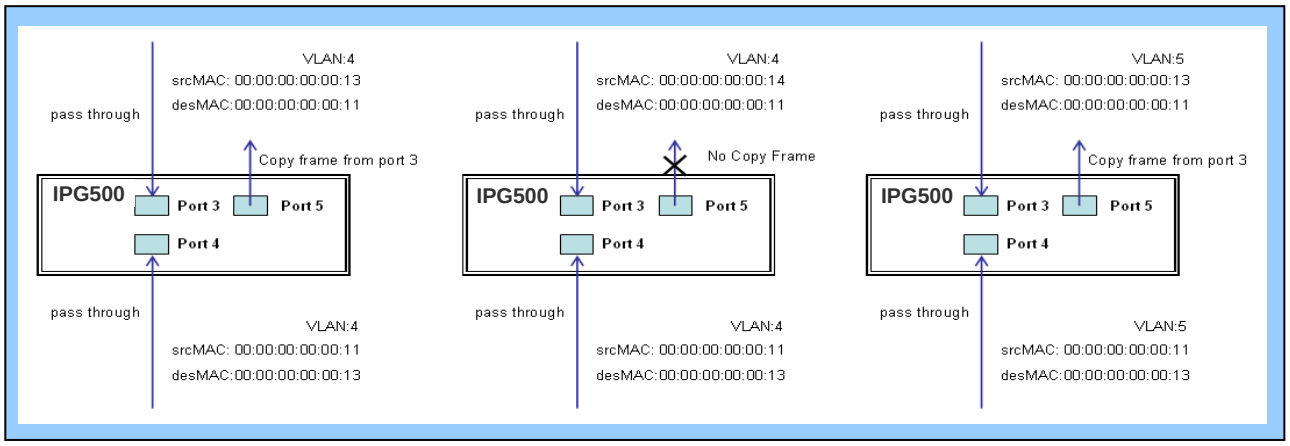
Step 2: Create a new ACL Entry rule under this ACL profile. (SrcMAC: 13 and DesMAC: 11)

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)***

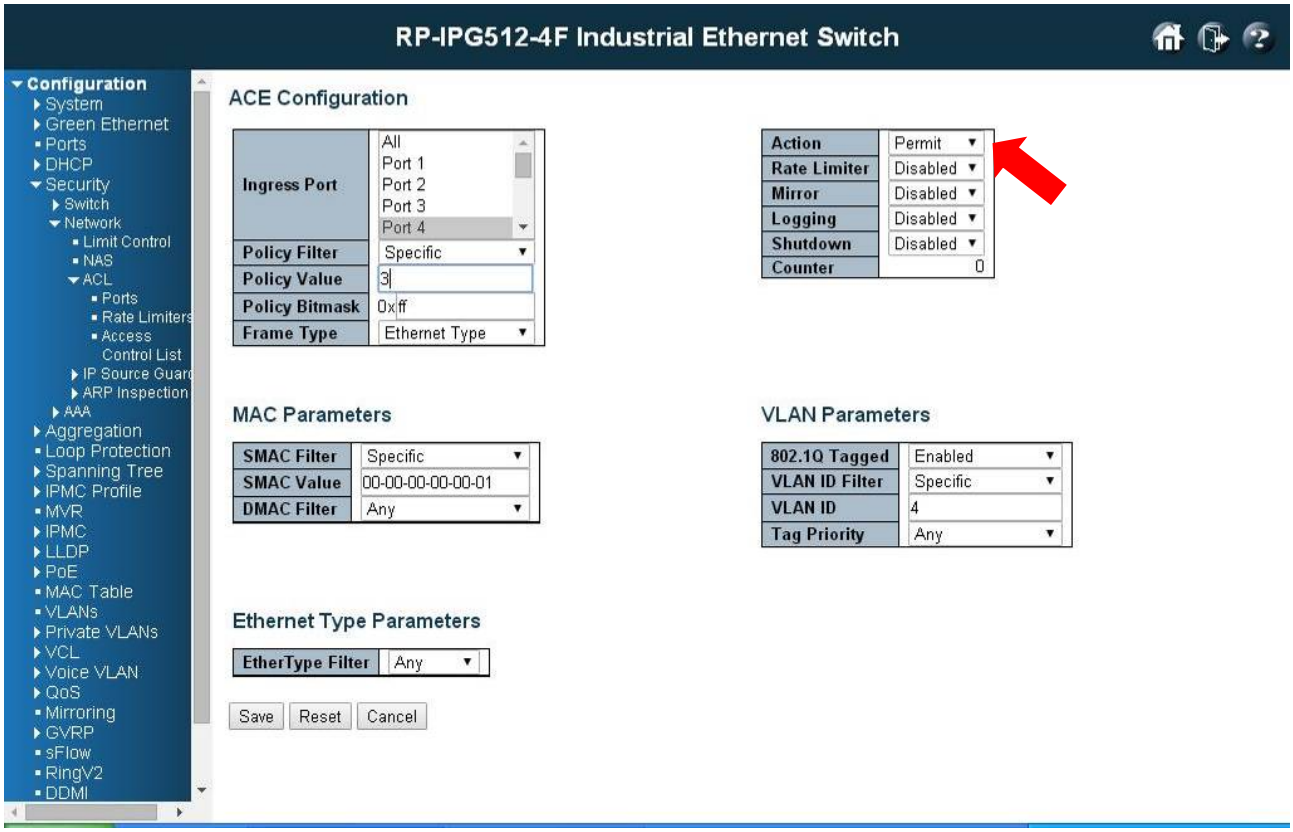
User can set default ACL Rule of GE port as “Deny”, then to bind a suitable profile with “Permit” action for ACL. It means GE port can not pass through all packets but ACL entry of the profile binding.

◎ One directional MAC address with one VLAN permit filtering.

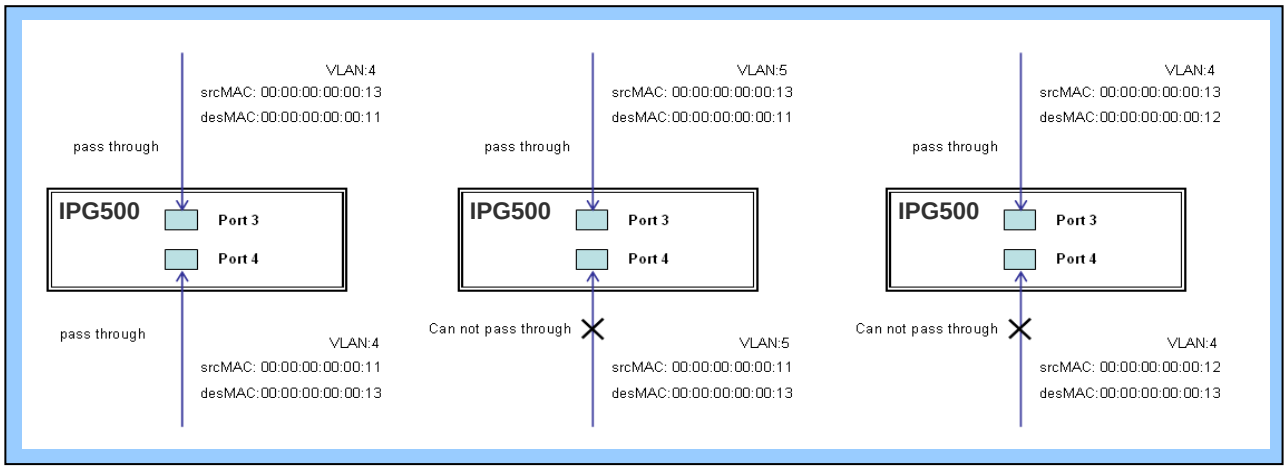
Step 1: Create a new ACL Profile. (Profile Name: AllowSomeMac)

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:

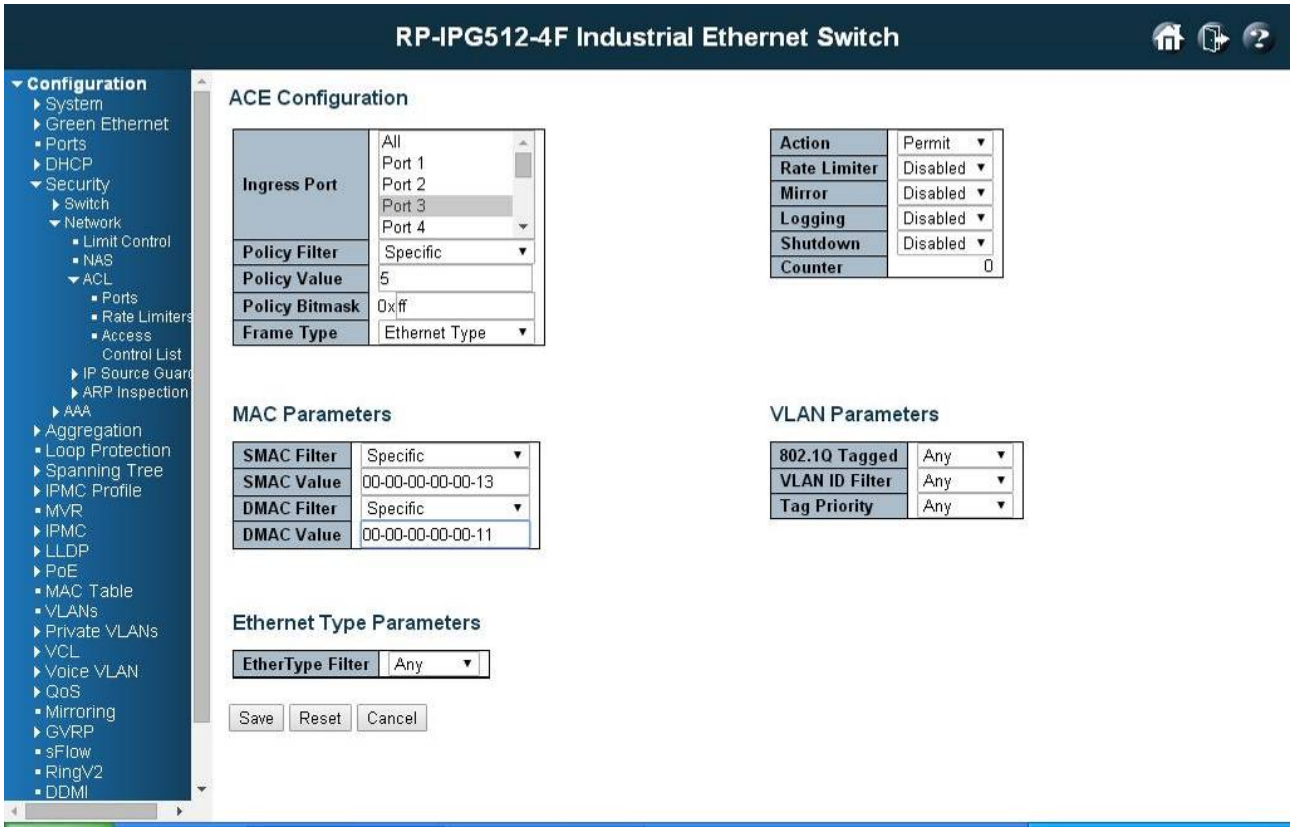
```
access-list ace 4 ingress interface GigabitEthernet 1/4 policy 3 tag tagged vid 4 frametype etype
smac 00-00-00-00-00-11
exit
  interface GigabitEthernet 1/3
  switchport trunk allowed vlan 4,5
  switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
  switchport trunk allowed vlan 4,5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

◎ Two directional MAC address with all VLAN permit filtering.

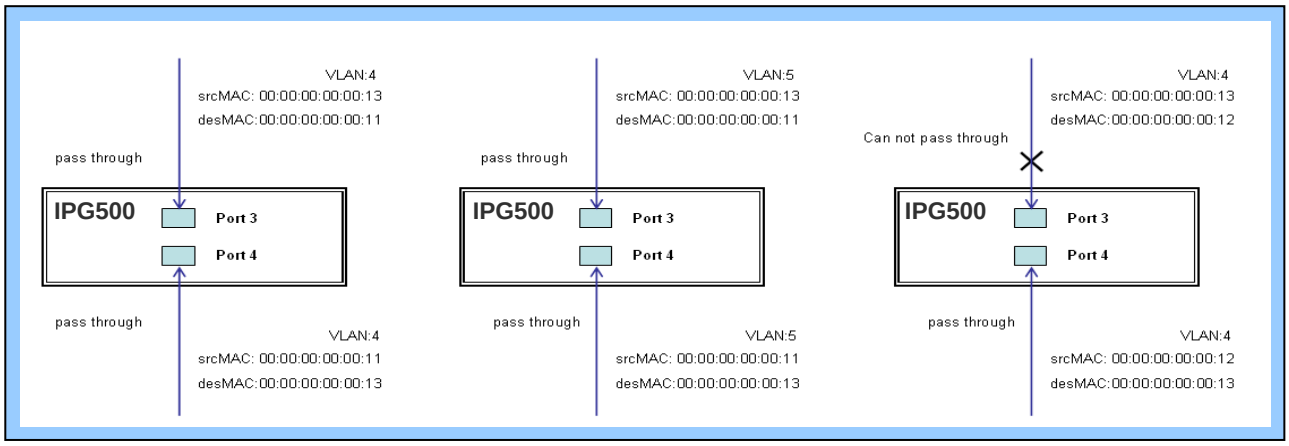
Step 1: Create a new ACL Profile. (Profile Name: AllowSomeMac)

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.

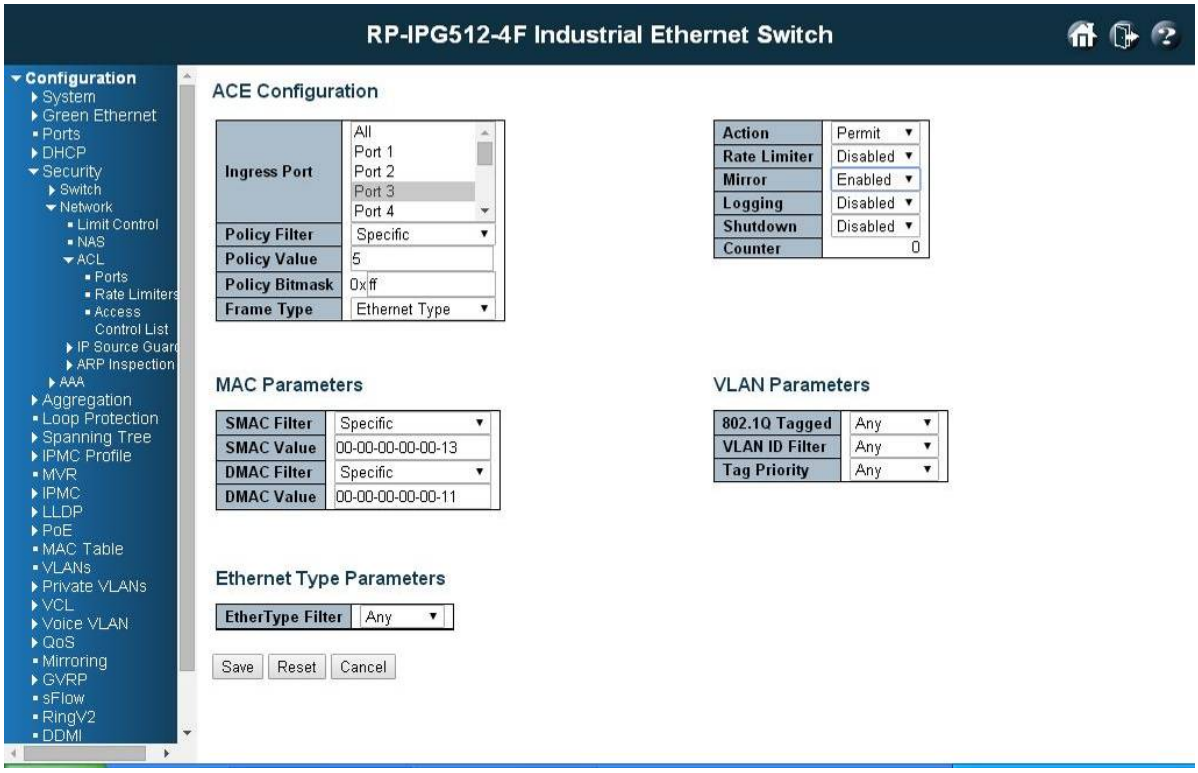
- **Case 1: (j)**

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)

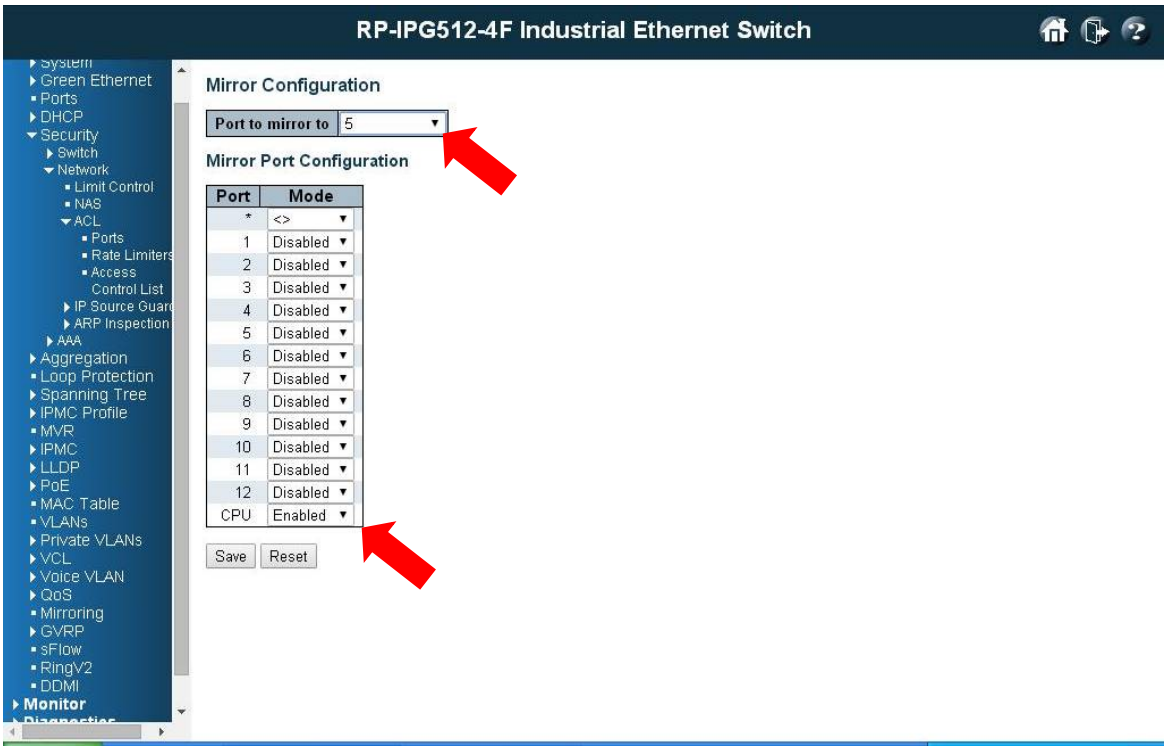
Step 1: Create a new ACL Profile. (Profile Name: CopyFrameTest)

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

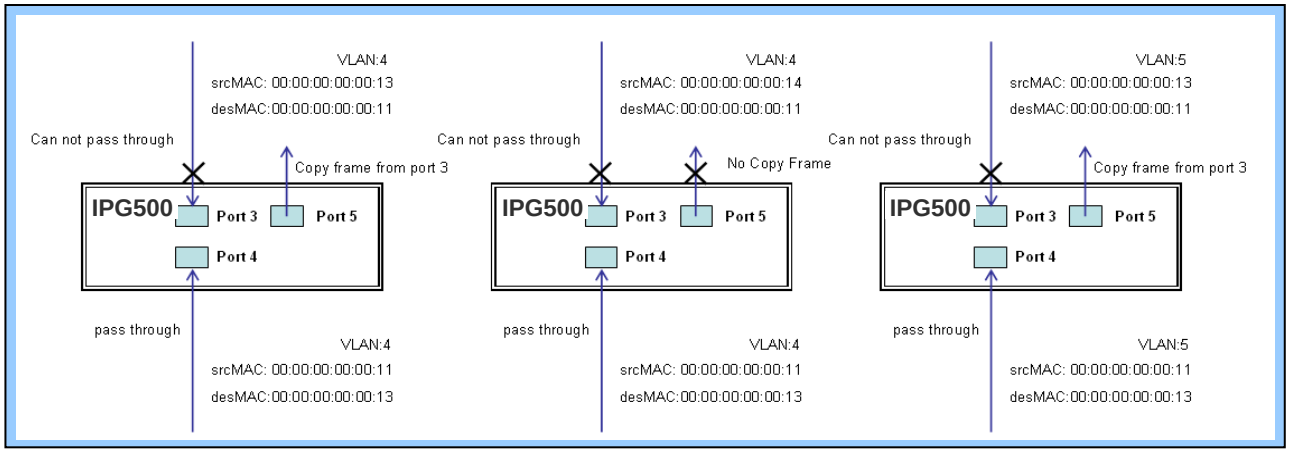


Step 3: Bind this ACL profile to a GE port. (PORT-3)

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.

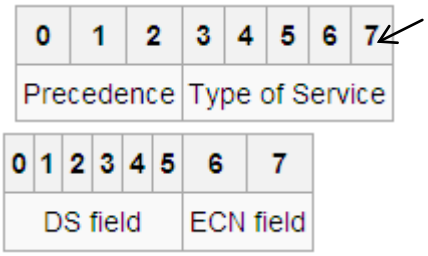
If user wants to filter only one directional IP address or L4 port, the other IP address and L4 port just set to all zero. It means don't care portion. The detail testing, please refer to MAC ACL above.

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.

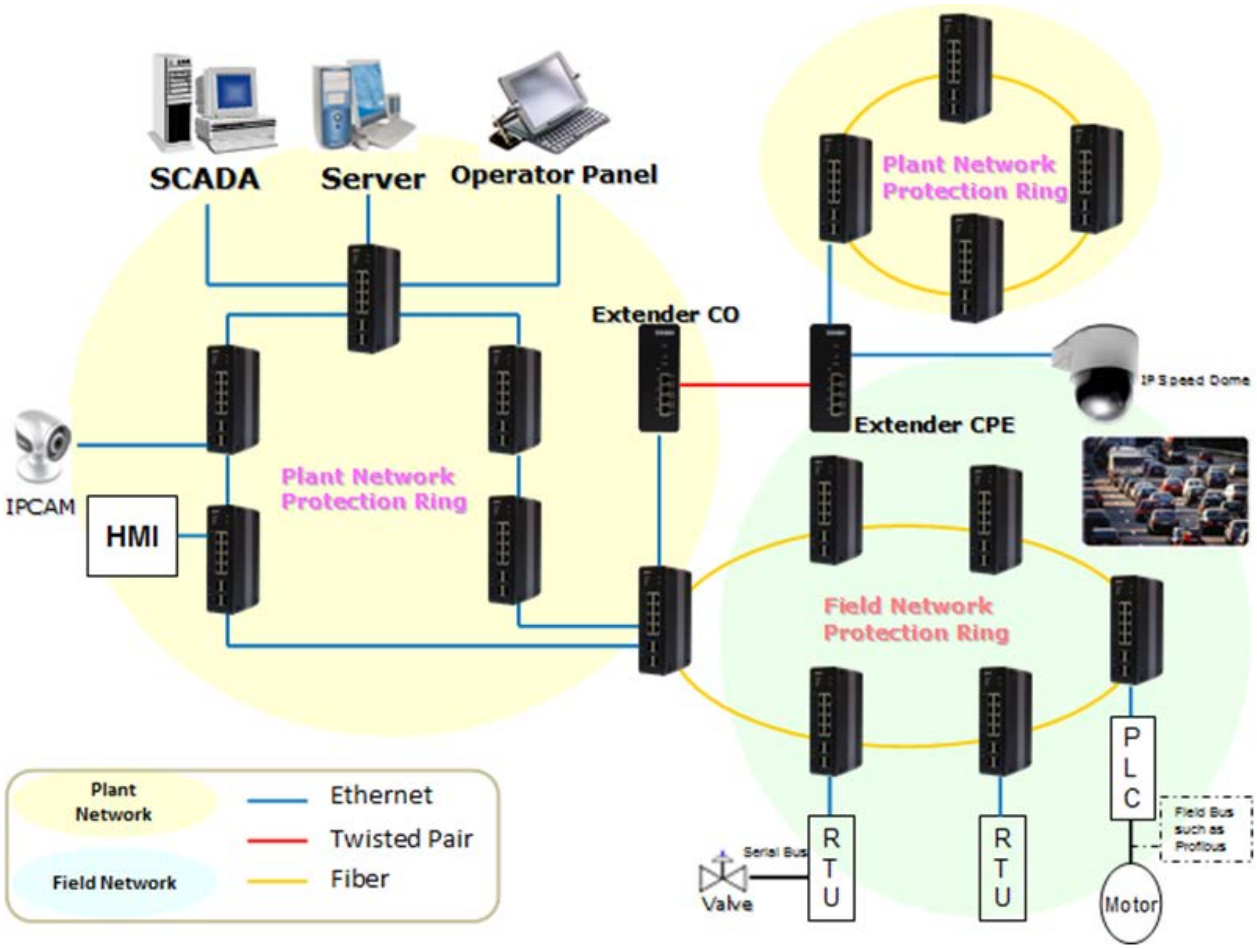
Valid Values: Precedence: 0~7, ToS: 0~15, DSCP: 0~63



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 IPG500 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.



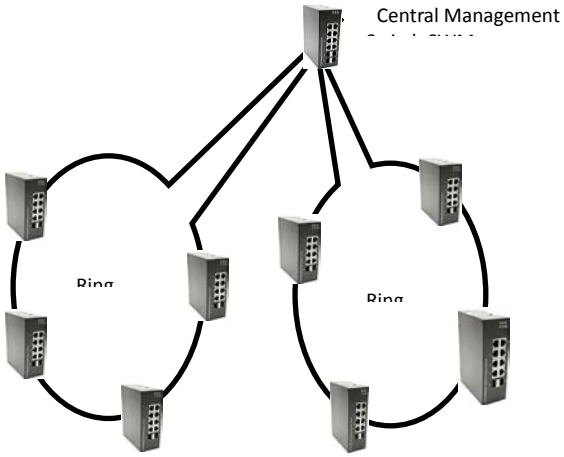
Ring Version 2 Feature

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.

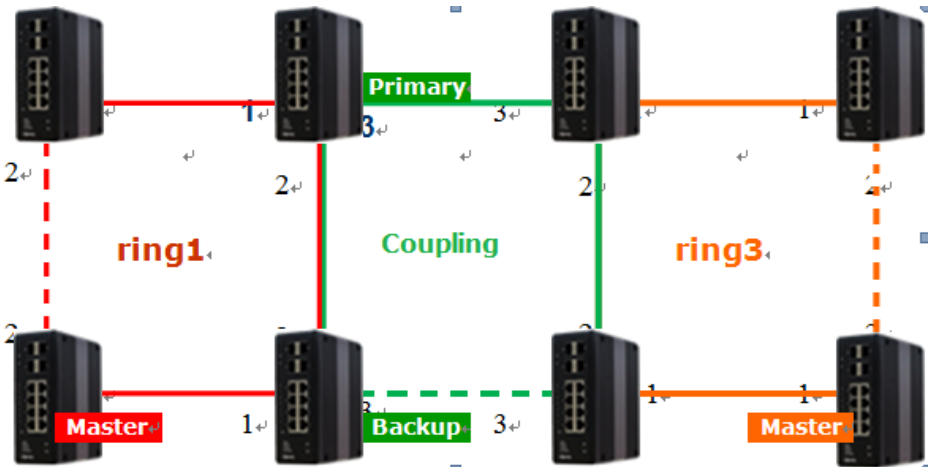
When role is ring/slave, both ring ports are forward port.



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

Ring - it could be master or slave.

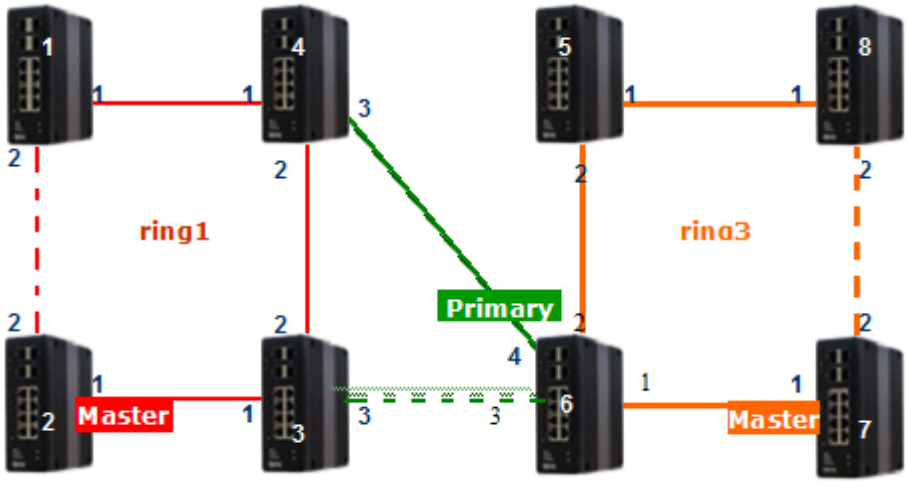
 # Coupling - it could be primary and backup.



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.

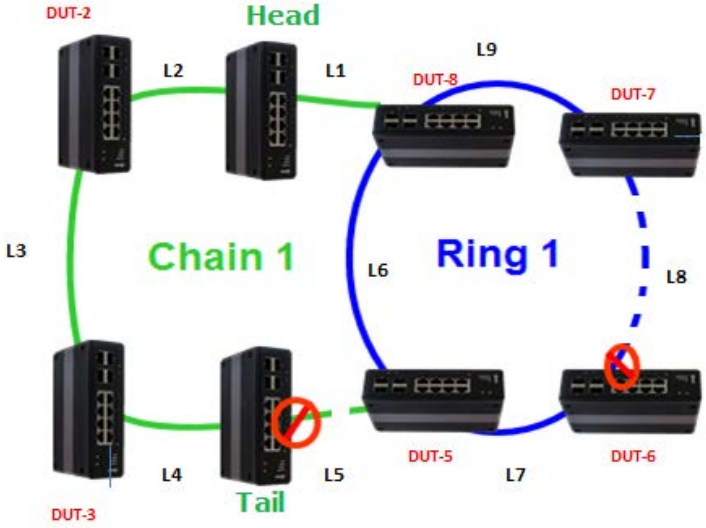
 # Dual-Homing



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.

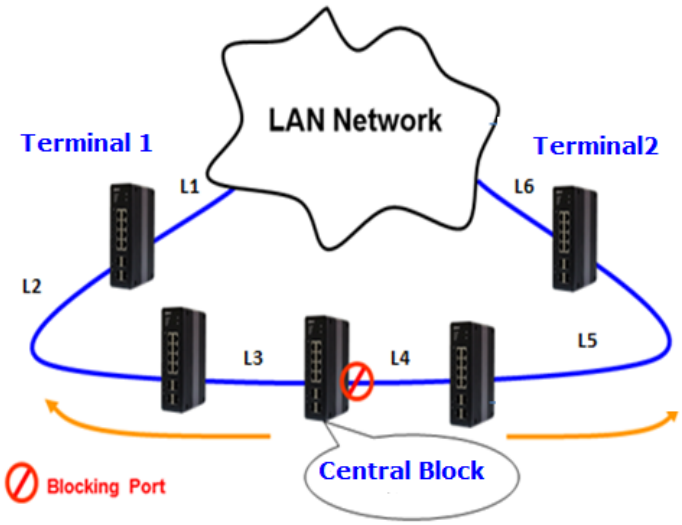


When role is chain/head, one ring port is head port and another is member port. Both ring ports are forwarded in normal state.

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 IPG500 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.

   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

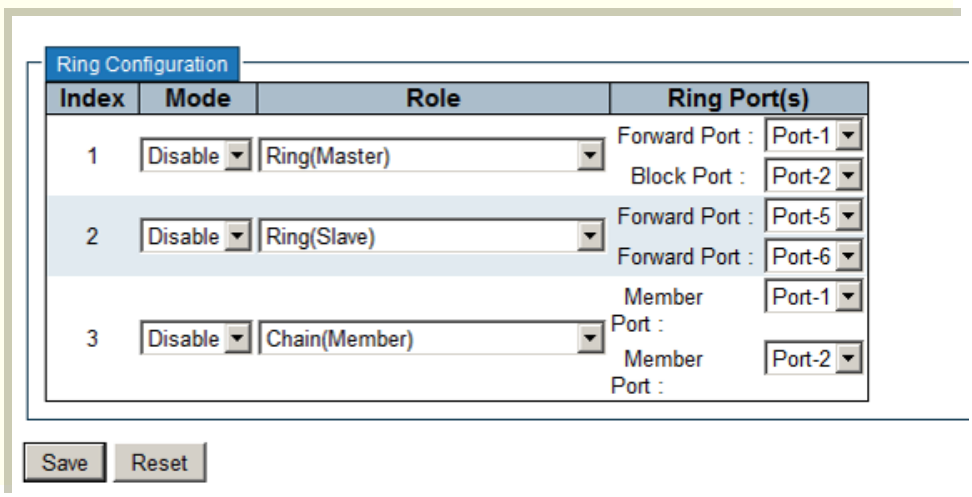
mode disable
node1 interface GigabitEthernet 1/1
node2 interface GigabitEthernet 1/2
role ring-master
mode enable

exit

Configuration (Web UI)

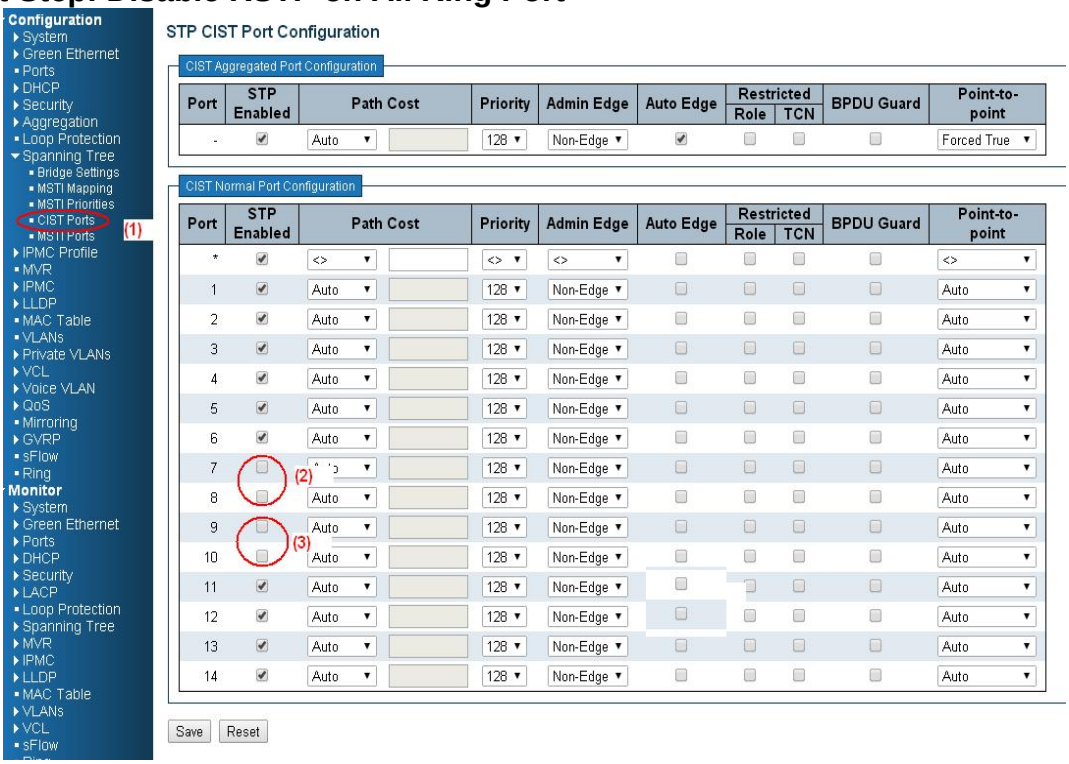
This document is introduction of the Industrial Ethernet Switch Software Spec for Ringv3.

In current design, one device supports 3 ring index, including Ring & Chain (single ring, dual ring, coupling, dual-homing, chain, and balancing-chain.)



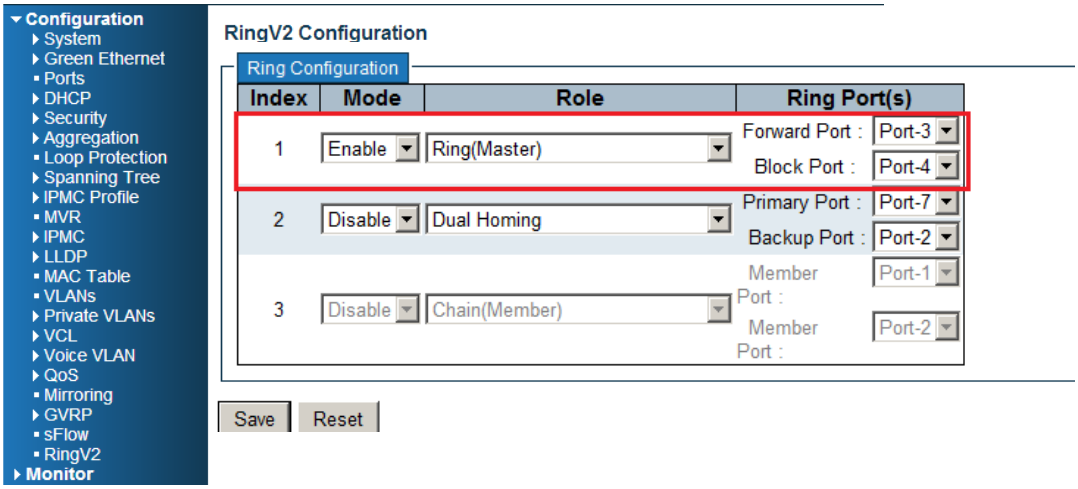
Note 1 - It must enable group1 before configure group2 as coupling.
Note 2 - When group1 or group2 is enabled, the configuration of group3 is invisible.
Note 3 - When group3 is enabled, the configuration of group1 and group3 is invisible.

First Step: Disable RSTP on All Ring Port



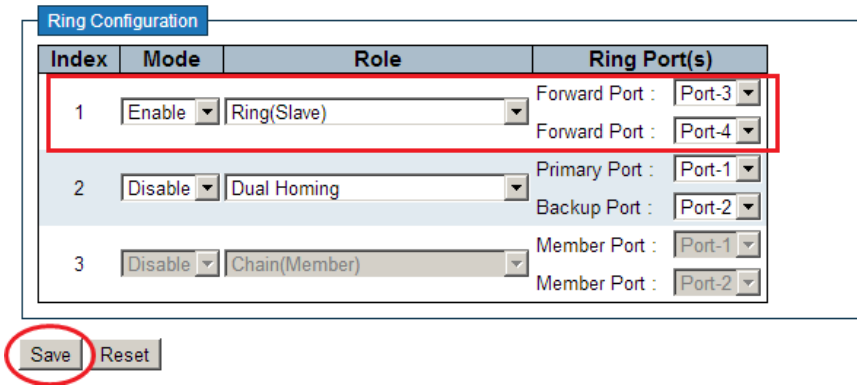
1. Go to “Configuration→Spanning Tree→ CIST ports” Web page
2. Do not enable STP global.
3. Click “Save” bottom

Ring Master



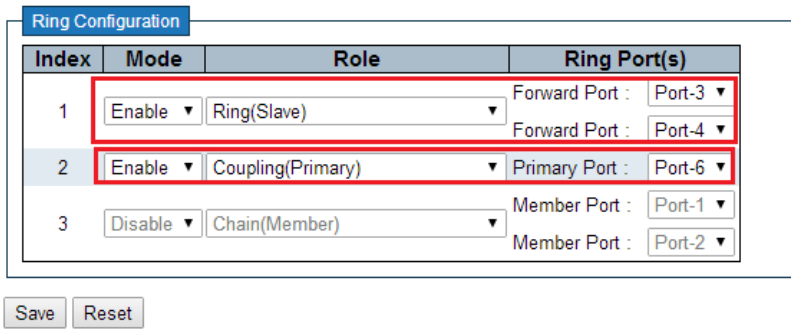
1. Go to “Configuration→ “RingV2” Web page
2. Enable Index1, and Select Role as Ring(Master)
3. Select one port as a “Forward Port”, another is “Block Port”

Ring Slave



1. Go to “Configuration→ “RingV2” Web page
2. Enable Index1, and Select Role as Ring(Slave)
3. Select two ports as “Forward Port”.

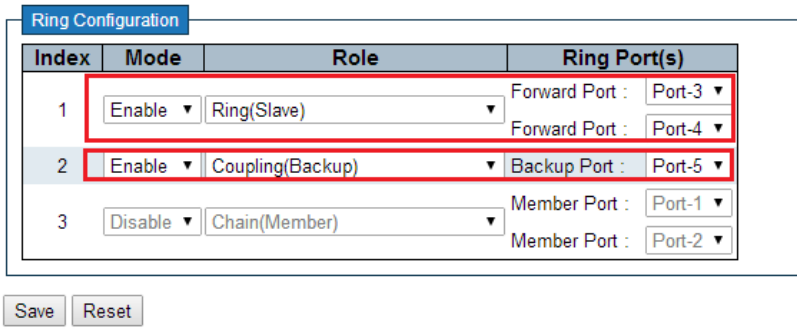
Coupling Primary



1. Go to “Configuration→ “RingV2” Web page
2. Enable Index1, and Select Role as Ring(Slave)
3. Select two ports as “Forward Port”.

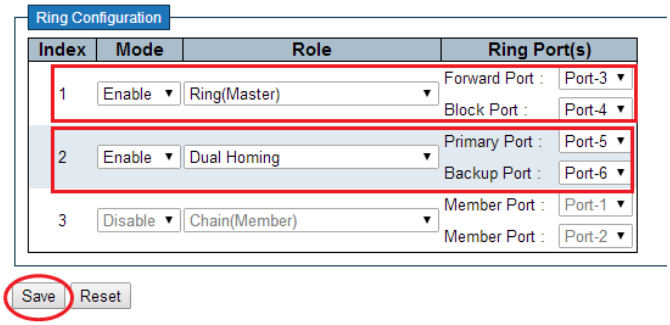
4. Enable Index2, and Select Role as “Coupling(Primary)”
5. Select one port as a “Primary Port”.

Coupling Backup



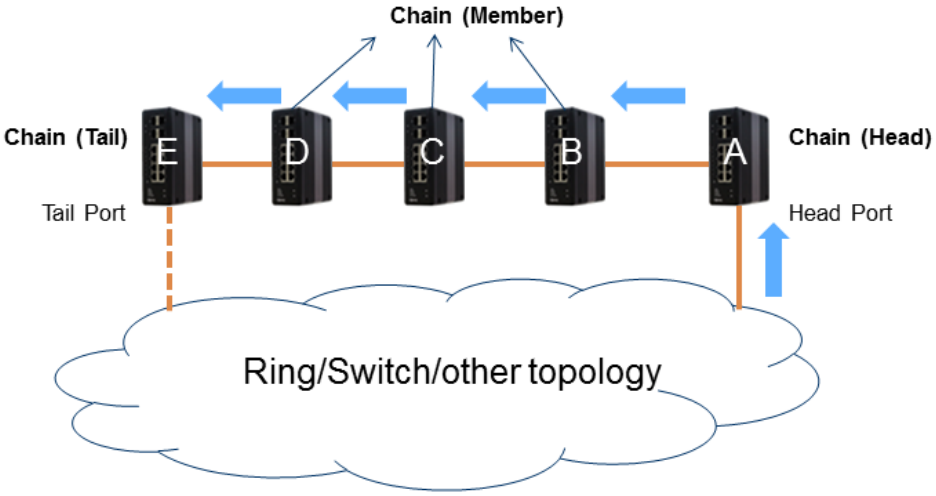
1. Go to “Configuration→ “RingV2” Web page
2. Enable Index1, and Select Role as Ring(Slave)
3. Select two ports as a “Forward Port”.
4. Enable Index2, and Select Role as “Coupling(Backup)”
5. Select one port as a “Backup Port”.

Dual-Homing

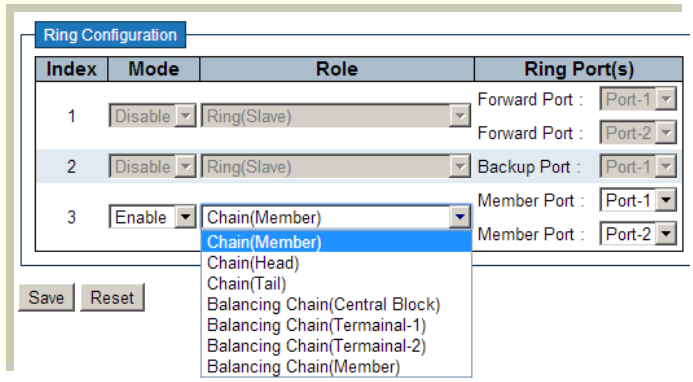


1. Go to “Configuration→ “RingV2” Web page
2. Enable Index1, and Select Role as Ring(Slave)
3. Select two ports as a “Forward Port”.
4. Enable Index2, and Select Role as “Dual Homing”
5. Select one port as a “Primary Port, and the other is “Backup Port”.

Chain Configuration

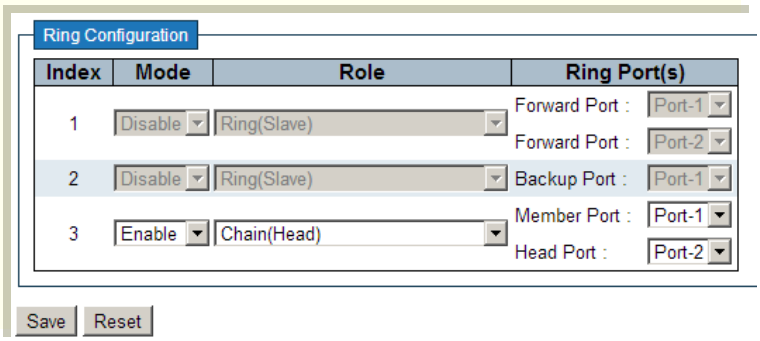


Chain - Member



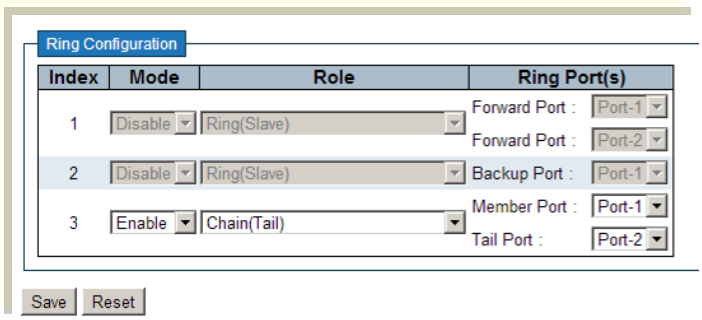
1. Go to “Configuration→ “RingV2” Web page
2. Disable Index1 and Index2, then enable Index3
3. Select Role to “Chain(Member)”
4. Select two member ports for this chain member switch.

Chain - Head



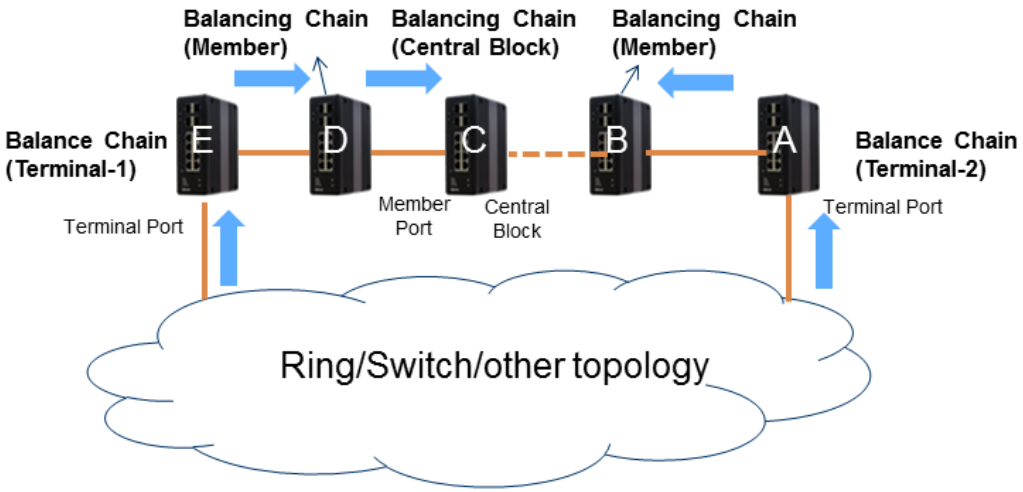
1. Go to “Configuration→ “RingV2” Web page
2. Disable Index1 and Index2, then enable Index3
3. Select Role to “Chain(Head)”
4. Select a member port and a head port for this chain head switch.

Chain - Tail

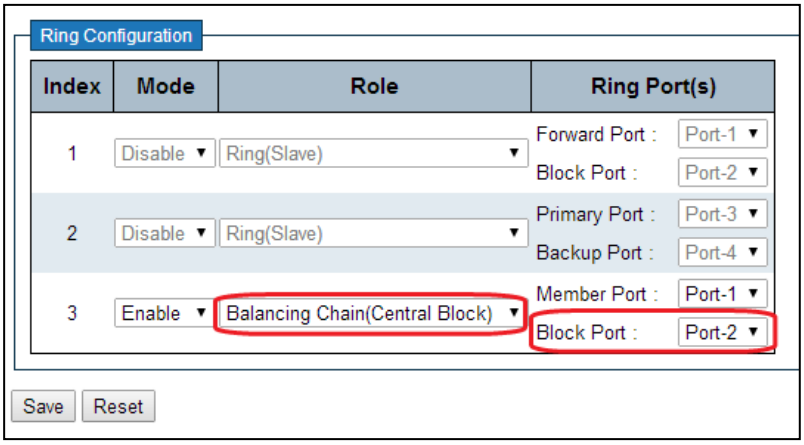


1. Go to “Configuration→ “RingV2” Web page
2. Disable Index1 and Index2, then enable Index3
3. Select Role to “Chain(Tail)”
4. Select a member port and a tail port for this chain tail switch.

Balance Chain Configuration



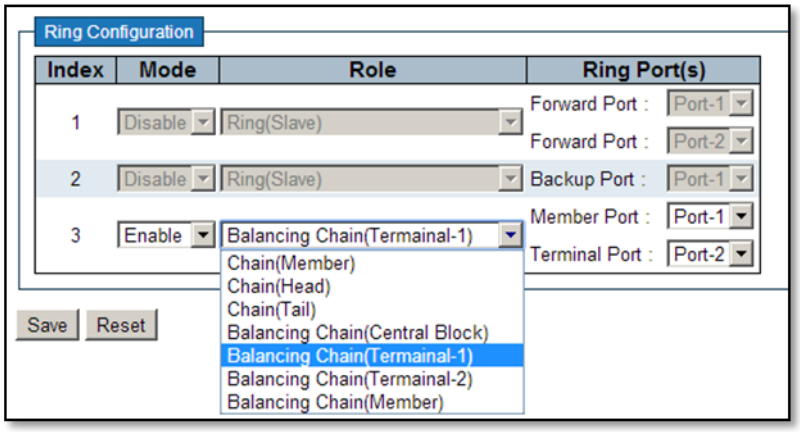
Balance Chain – Central Block



1. Go to “Configuration→ “RingV2” Web page
2. Disable Index1 and Index2, then enable Index3
3. Select Role to “Balancing Chain(Central Block)”

4. Select a member port and a block port for this central block switch.

Balance Chain –Terminal-1 and -2



1. Go to “Configuration→ “RingV2” Web page
2. Disable Index1 and Index2, then enable Index3
3. Select Role to “Balancing Chain(Terminal-1 or -2)”
4. Select a member port and a terminal port for this balancing chain terminal switch.

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

The KGS 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 shape parameter on every VLAN priority for Ethernet interface. Currently KGS supports Strict Priority and SP+WRR(Weighted Round Robin) scheduling methods on each port. Please find the detail reference on IPG500 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
SPQ	SPQ	SPQ	SPQ	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.

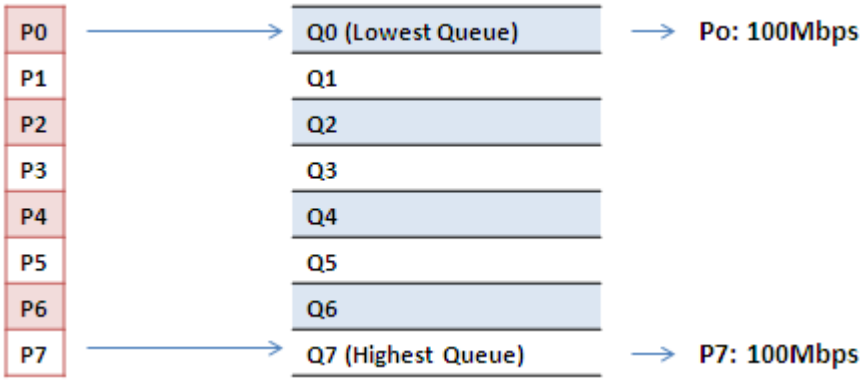
Example 1: SPQ without Shaping (Default profile)

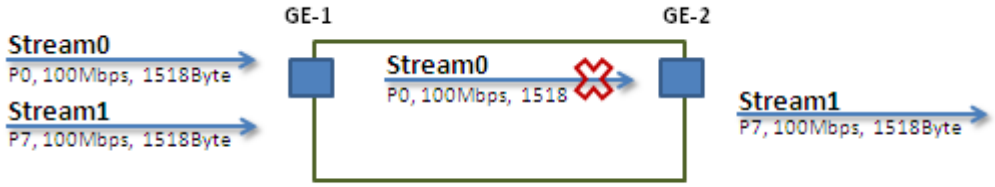
We send 2 Streams (Stream0, Stream1) from PORT-1 to PORT-2. Both 2 Streams each have 100Mbps. Stream0 includes VLAN Priority0, Stream1 includes VLAN Priority7. Set PORT-2 link speed to 100Mbps.

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 IPG500.

Gigabit port VLAN Priority & Queue mapping:



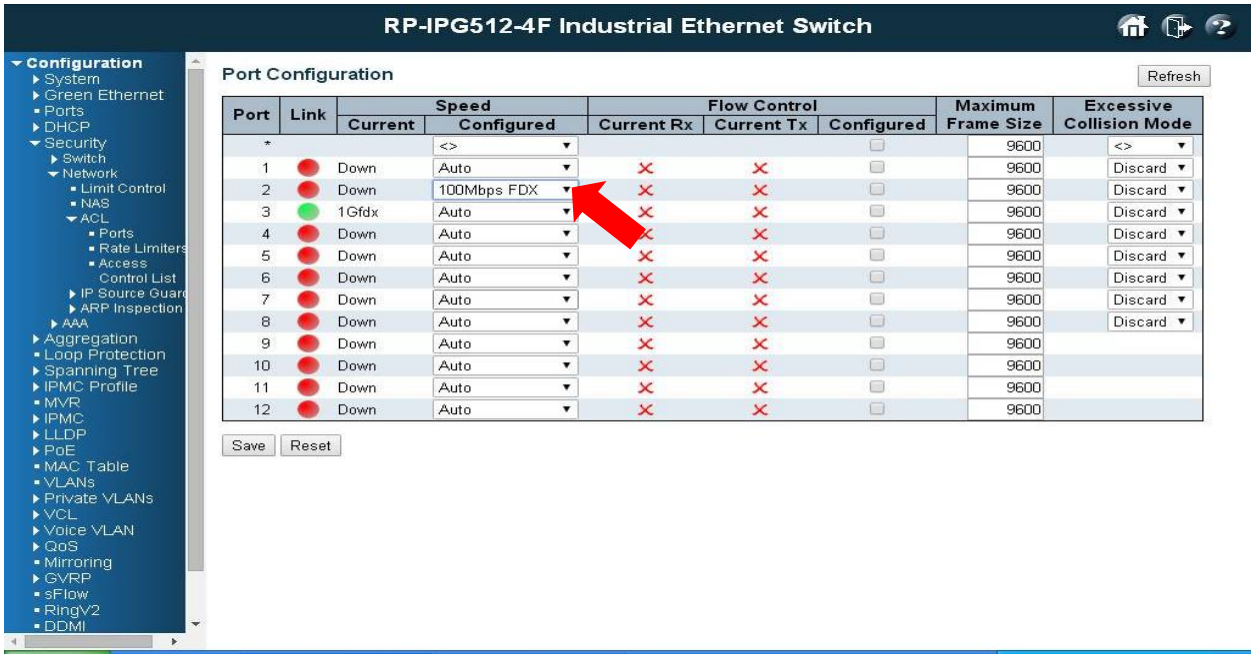


- **Stream0 :**
  Dst Mac : 00:00:00:00:20:01
  Src Mac : 00:00:00:00:10:01
  Vlan : 100
  Vlan prio : 0
  Send rate : 100Mbps
  Packet length: 1518bytes

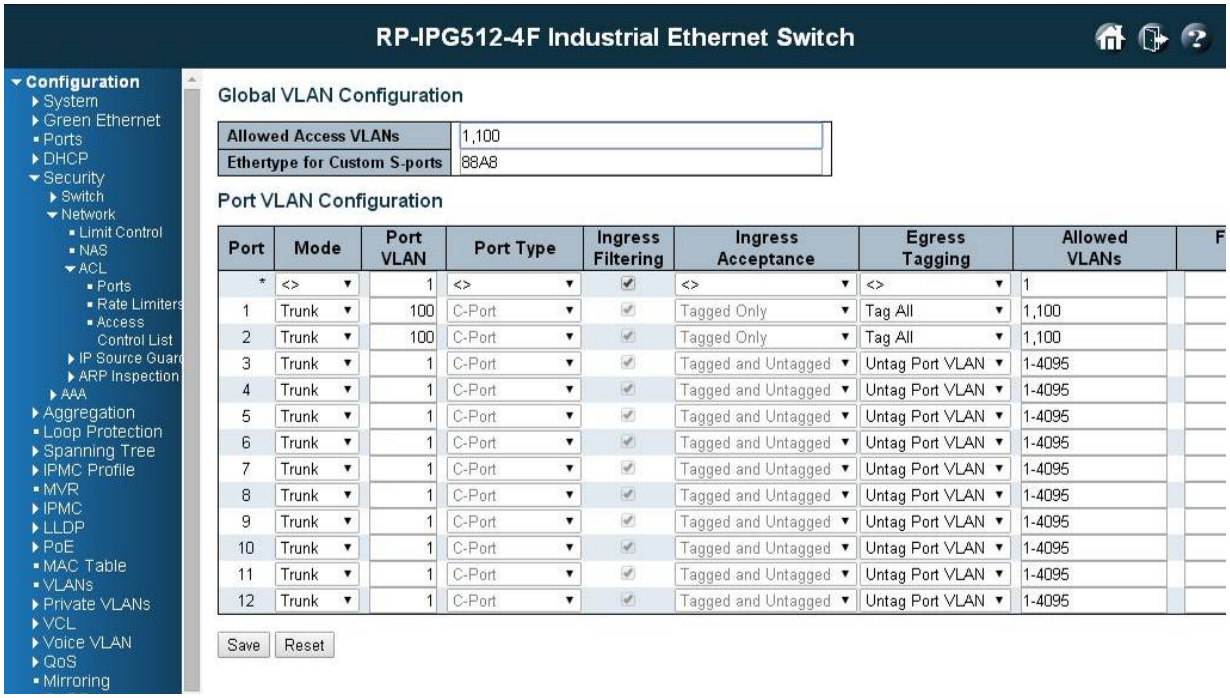
- **Stream1**:
  Dst Mac : 00:00:00:00:20:02
  Src Mac : 00:00:00:00:10:02
  Vlan : 100
  Vlan prio : 7
  Send rate : 100Mbps
  Packet length: 1518bytes

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 1/1
  switchport trunk native vlan 100
  switchport trunk allowed vlan 1,100
  switchport trunk vlan tag native
  switchport mode trunk
!
interface GigabitEthernet 1/2
  switchport trunk native vlan 100
  switchport trunk allowed vlan 1,100
  switchport trunk vlan tag native
  switchport mode trunk
```

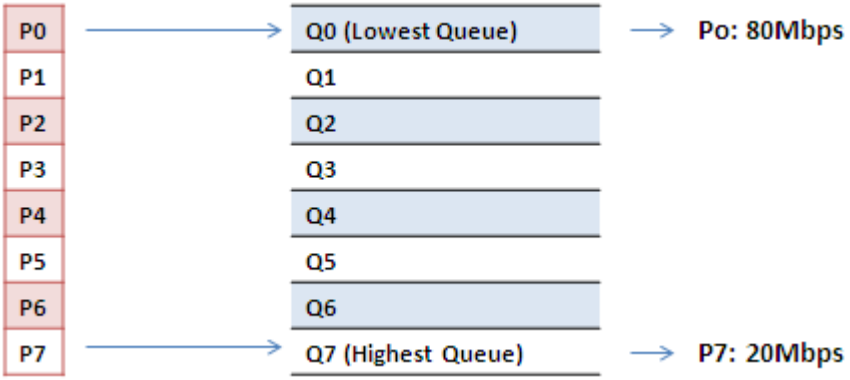
Example 2: SPQ with Shaping

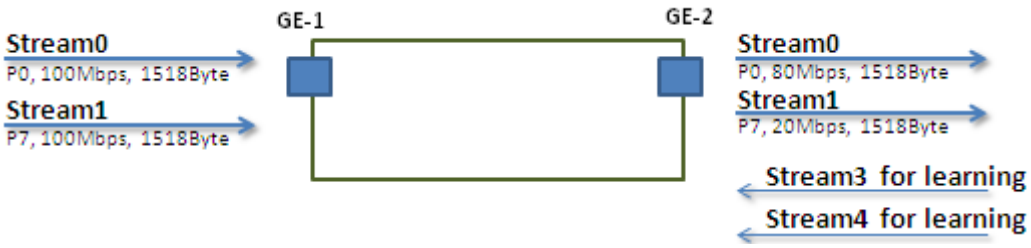
We send 2 Streams (Stream0, Stream1) from port1 to port-2. Both 2 Streams each have 100Mbps. Stream0 includes VLAN Priority0, Stream1 includes VLAN Priority7. Stream3 and Stream4 only for learning which make sure the traffic are not flooding.

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 IPG500.

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

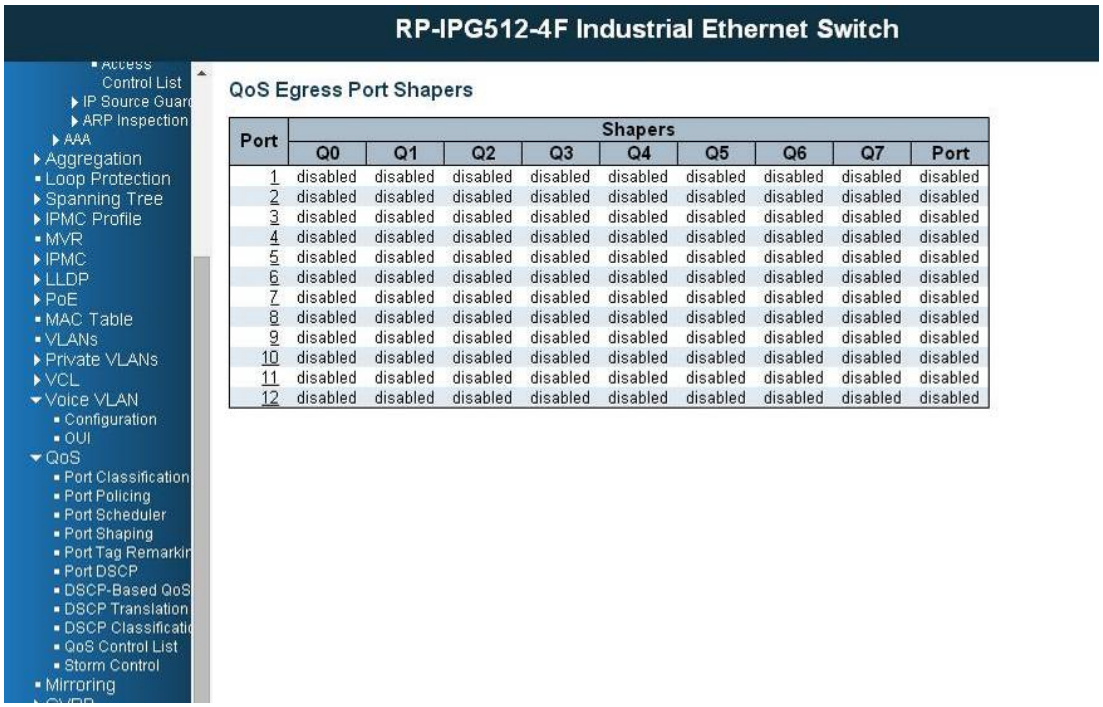
- **Stream1**:
  Dst Mac : 00:00:00:00:20:02
  Src Mac : 00:00:00:00:10:02
  Vlan : 100
  Vlan prio : 7
  Send rate : 100Mbps
  Packet length: 1518bytes

- **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

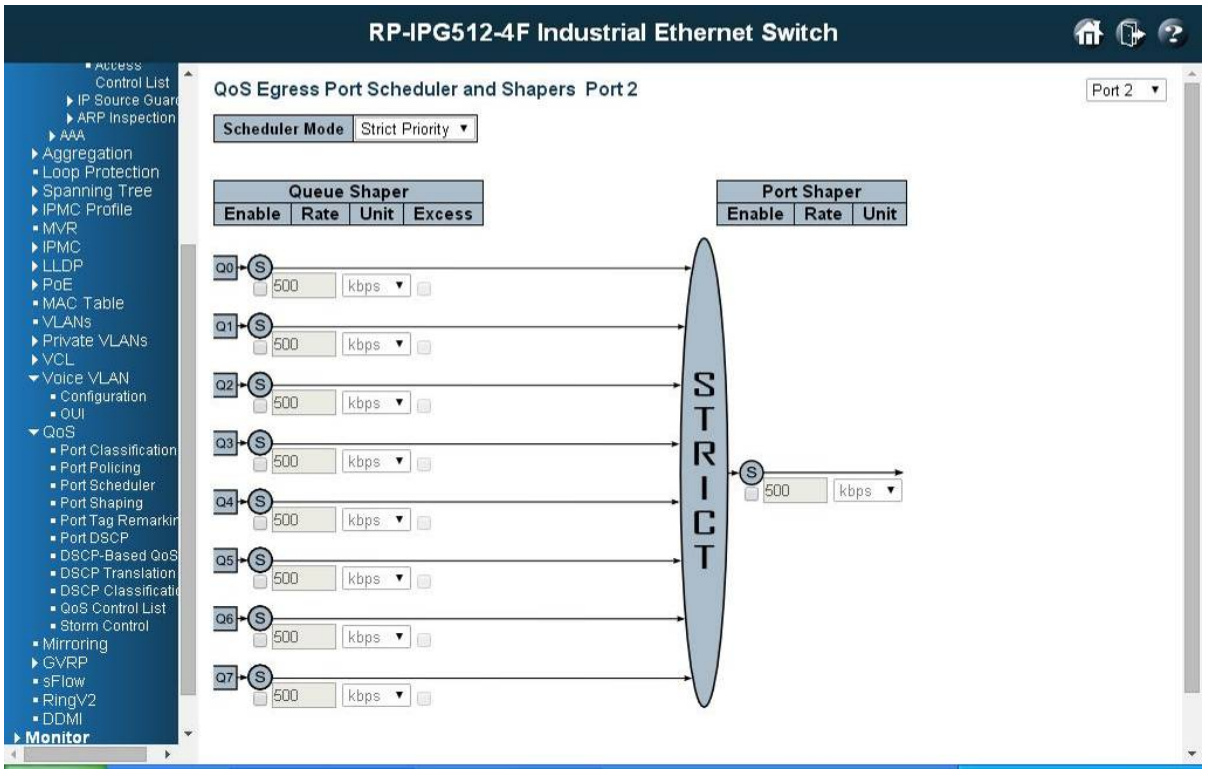
- **Stream4 : (for Learning)**
  Dst Mac : 00:00:00:00:10:02
  Src Mac : 00:00:00:00:20:02
  Vlan : 100
  Vlan prio : 0
  Send rate : 10Mbps
  Packet length: 1518bytes

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.

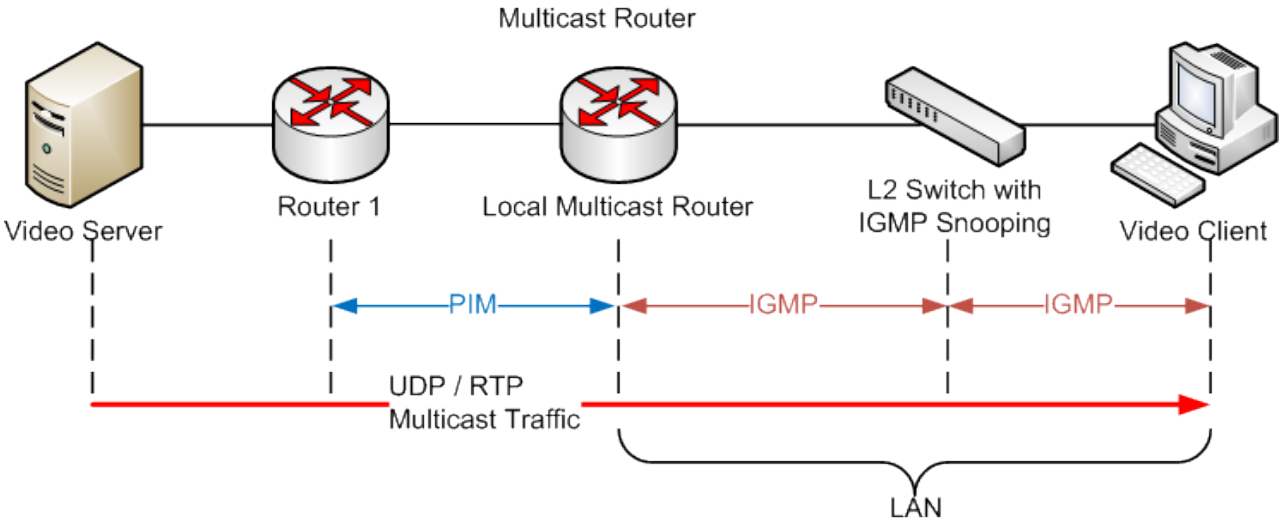


CLI configuration command:

```
interface GigabitEthernet 1/2
  switchport trunk native vlan 100
  switchport trunk allowed vlan 1,100
  switchport trunk vlan tag native
  switchport mode trunk
  qos queue-shaper queue 0 80000
  qos queue-shaper queue 7 20000
```

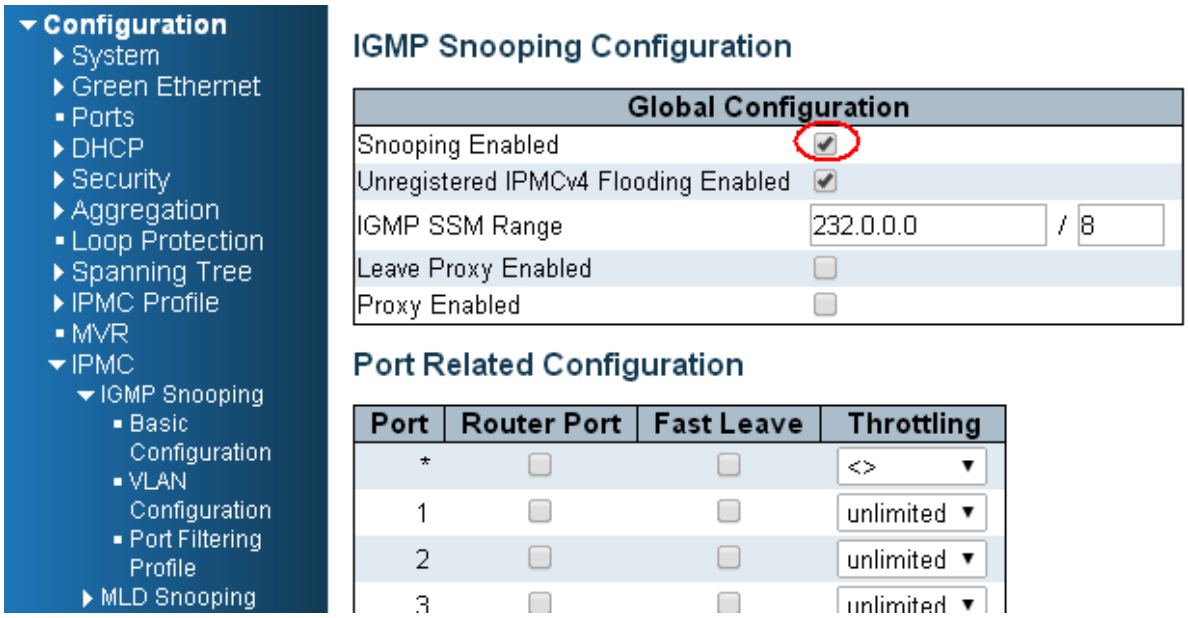
IGMP Application Guide

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.

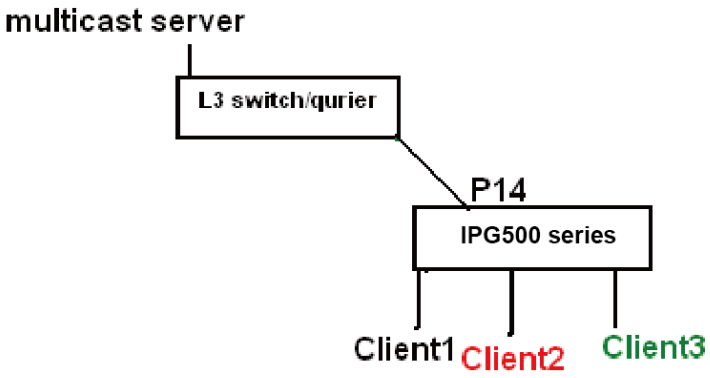


Example 1:

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.

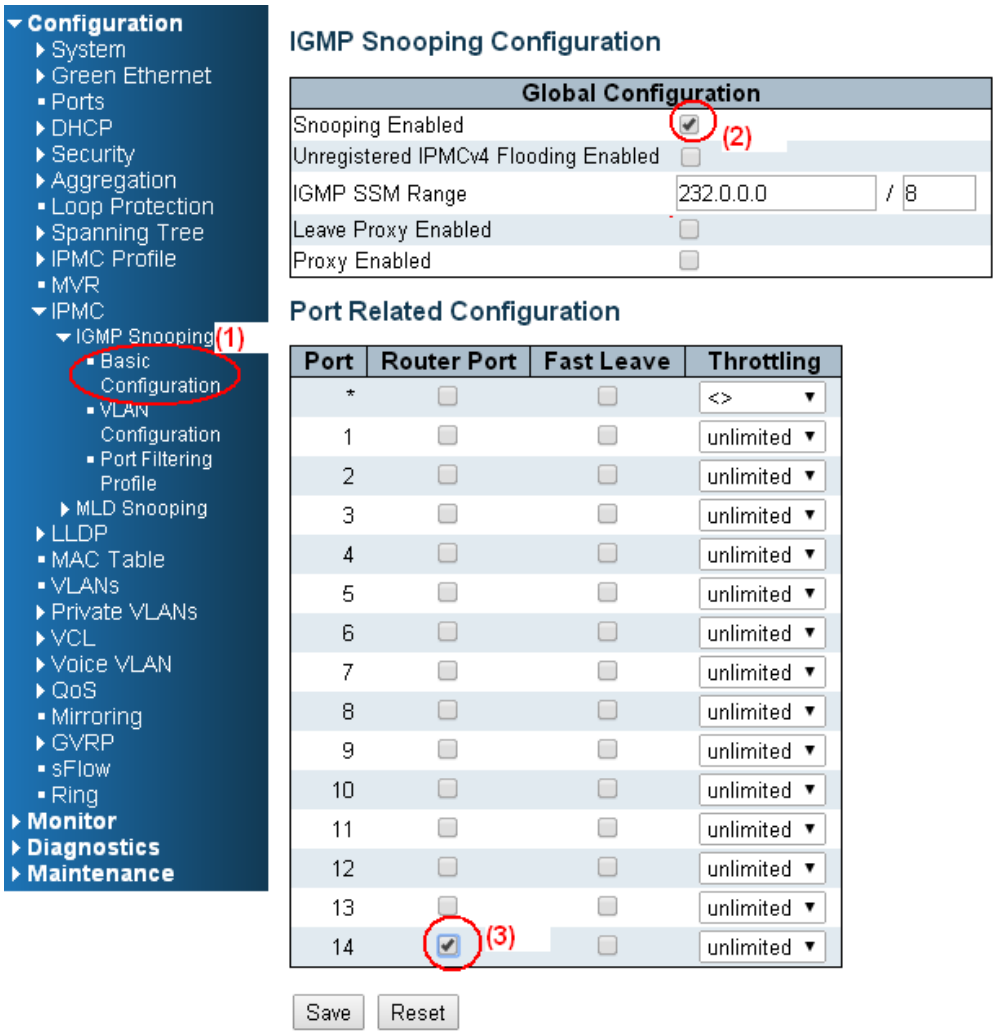

Configuration
System
Green Ethernet
Ports
DHCP
Security
Aggregation
Loop Protection
Spanning Tree
IPMC Profile
MVR
IPMC
IGMP Snooping
Basic Configuration
VLAN Configuration
Port Filtering Profile
MLD Snooping
IGMP Snooping Configuration
Global Configuration
Snooping Enabled
Unregistered IPMCv4 Flooding 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:

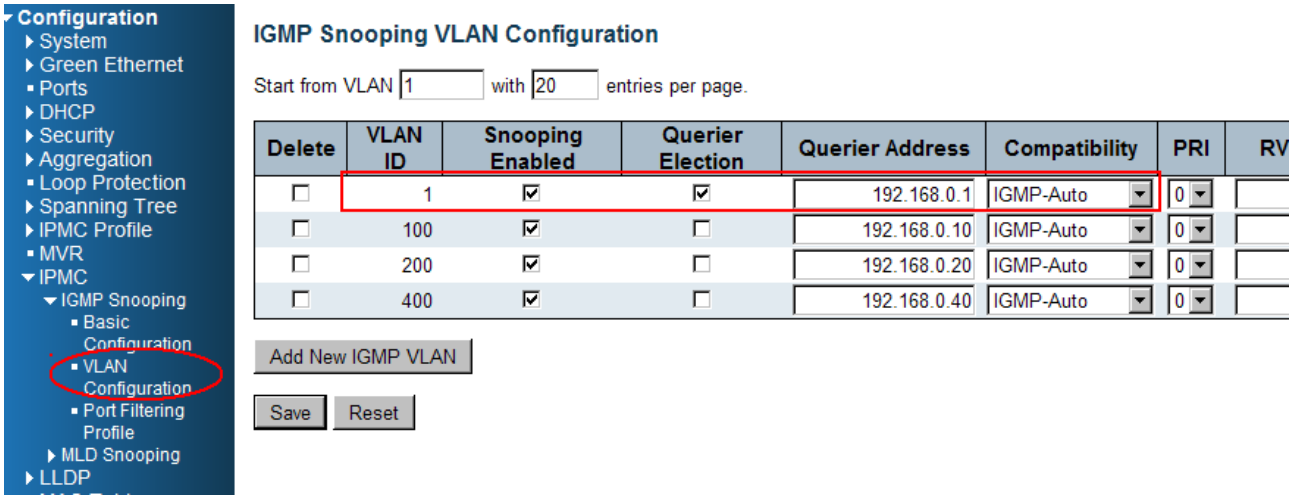


1. Go to “Configuration→IPMC→Basic Configuration” to select the check box of “Snooping Enable”
2. Un-select the check box of ”Unregistered IPMCv4 Flooding Enabled”
3. If Multicast stream is from L3 switch, then the uplink port have to be “Router Port”

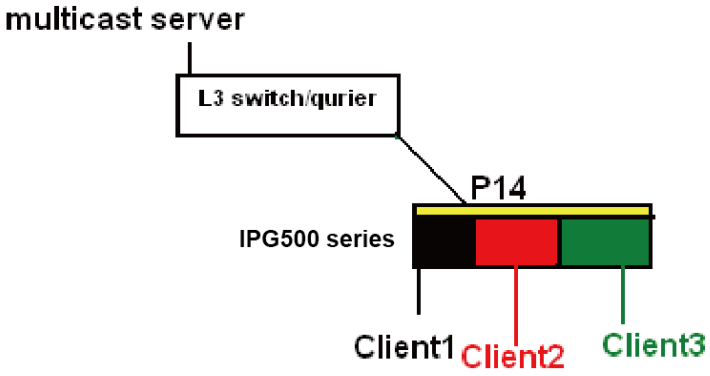
Notice: If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.



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

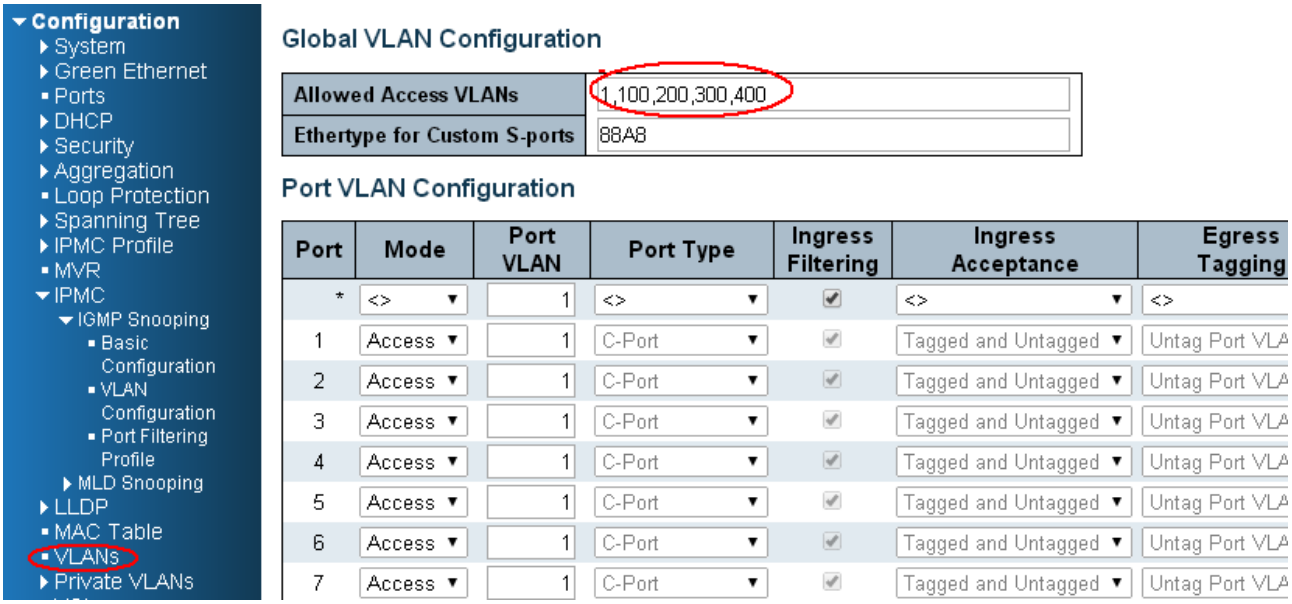

Configuration
System
Green Ethernet
Ports
DHCP
Security
Aggregation
Loop Protection
Spanning Tree
IPMC Profile
MVR
IPMC
IGMP Snooping
Basic Configuration
VLAN Configuration
Port Filtering Profile
MLD Snooping
LLDP
IGMP Snooping VLAN Configuration
Start from VLAN 1 with 20 entries per page.
Delete
VLAN ID
Snooping Enabled
Querier Election
Querier Address
Compatibility
PRI
RV
1
192.168.0.1
IGMP-Auto
0
100
192.168.0.10
IGMP-Auto
0
200
192.168.0.20
IGMP-Auto
0
400
192.168.0.40
IGMP-Auto
0
Add New IGMP VLAN
Save
Reset

Example3:

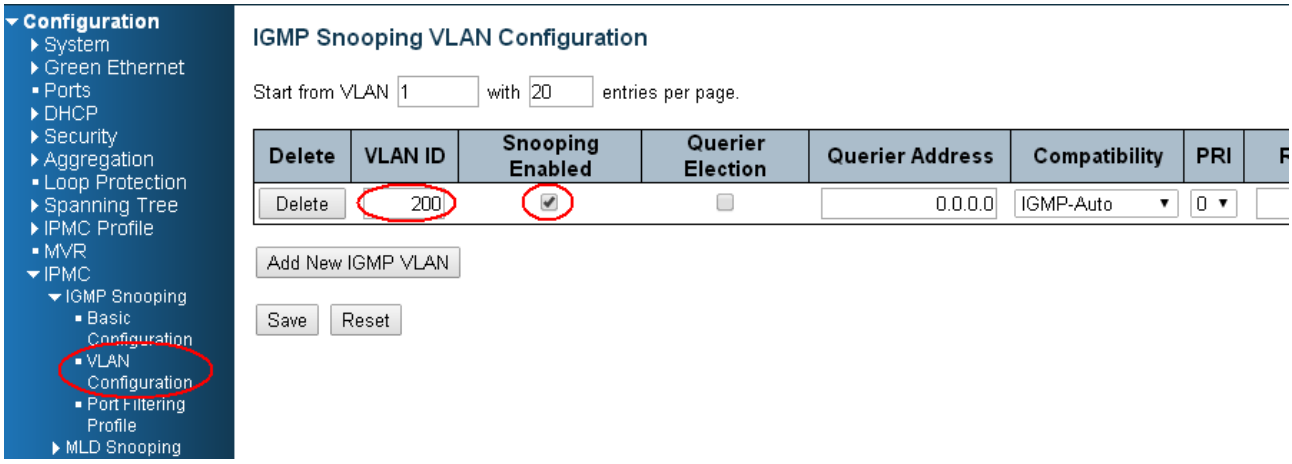


In this scenario, these clients belong to multiple vlans, you have to create more one vlan to be the agent for all client vlans.

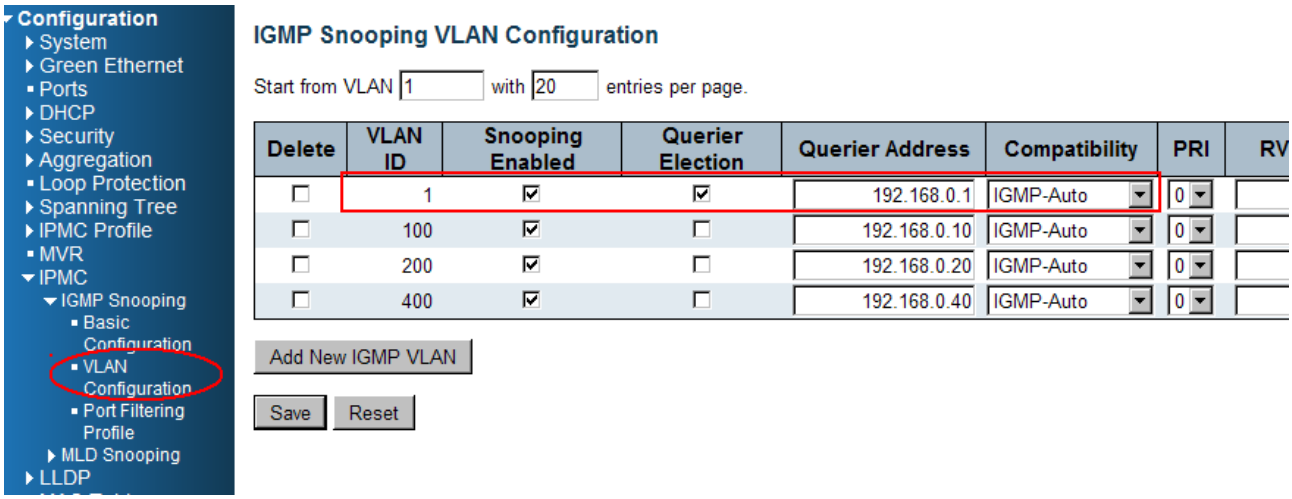
1. To create a vlan : go to ”Configuration→VLANs→Allow Access VLANs”, then set port 14 be vlan200 member port.



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



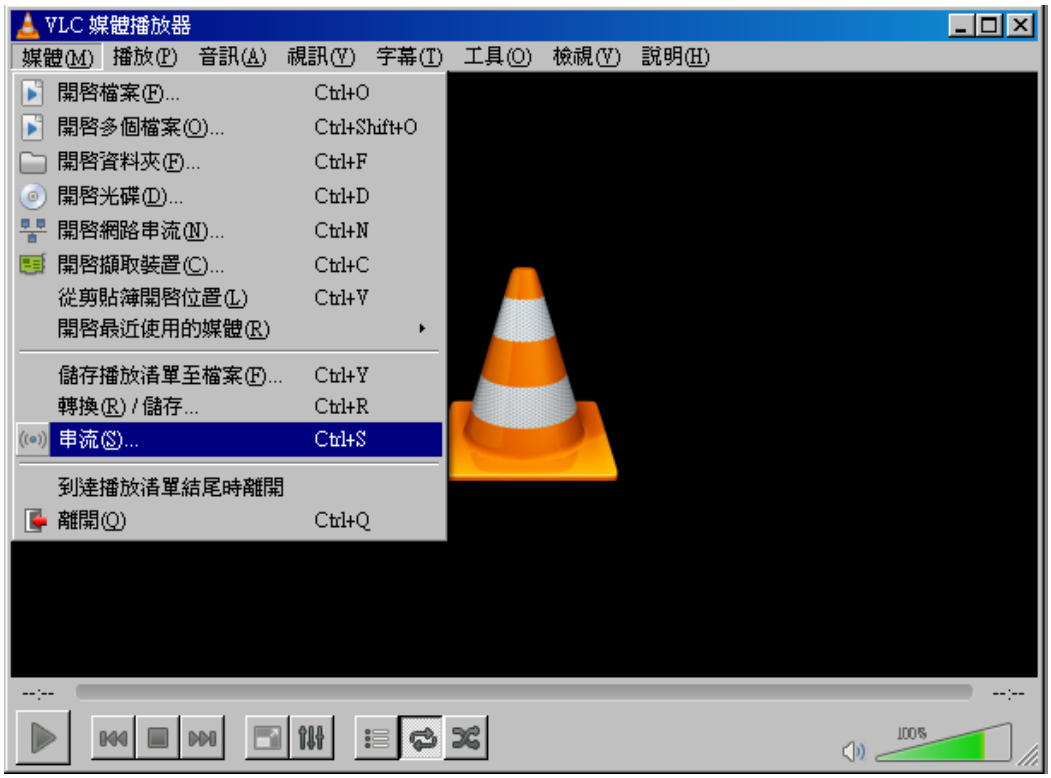
3. If there is no querier on the L3 switch, you have to select “Querier Election”, and set the “Querier Address ”, the IP address is in the same network as uplink interface.
4. Selecet the IGMP version as server.



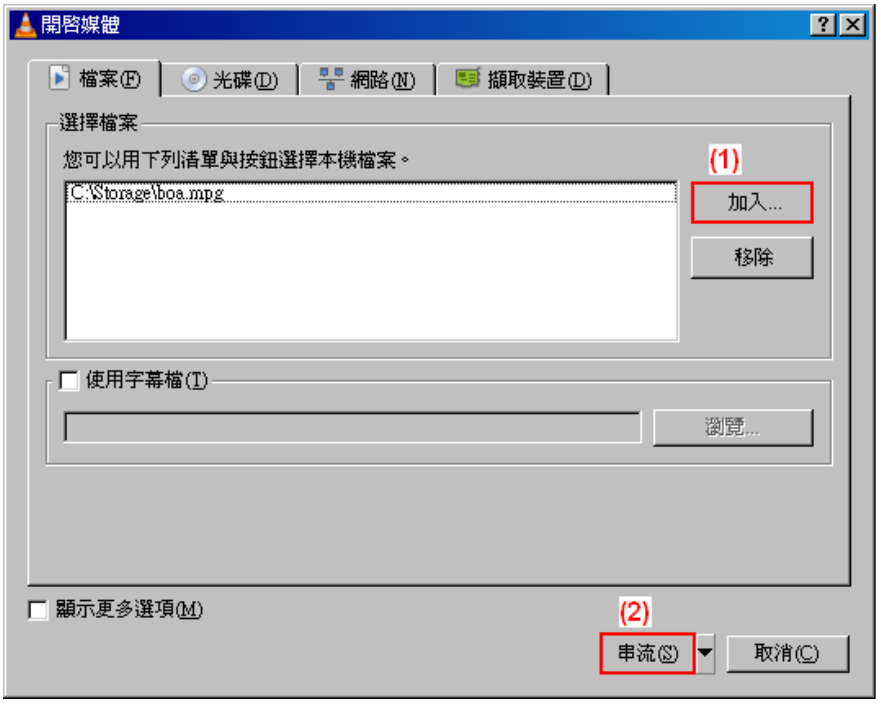
How to Configuration VLC

VLC Configure on IGMP Server

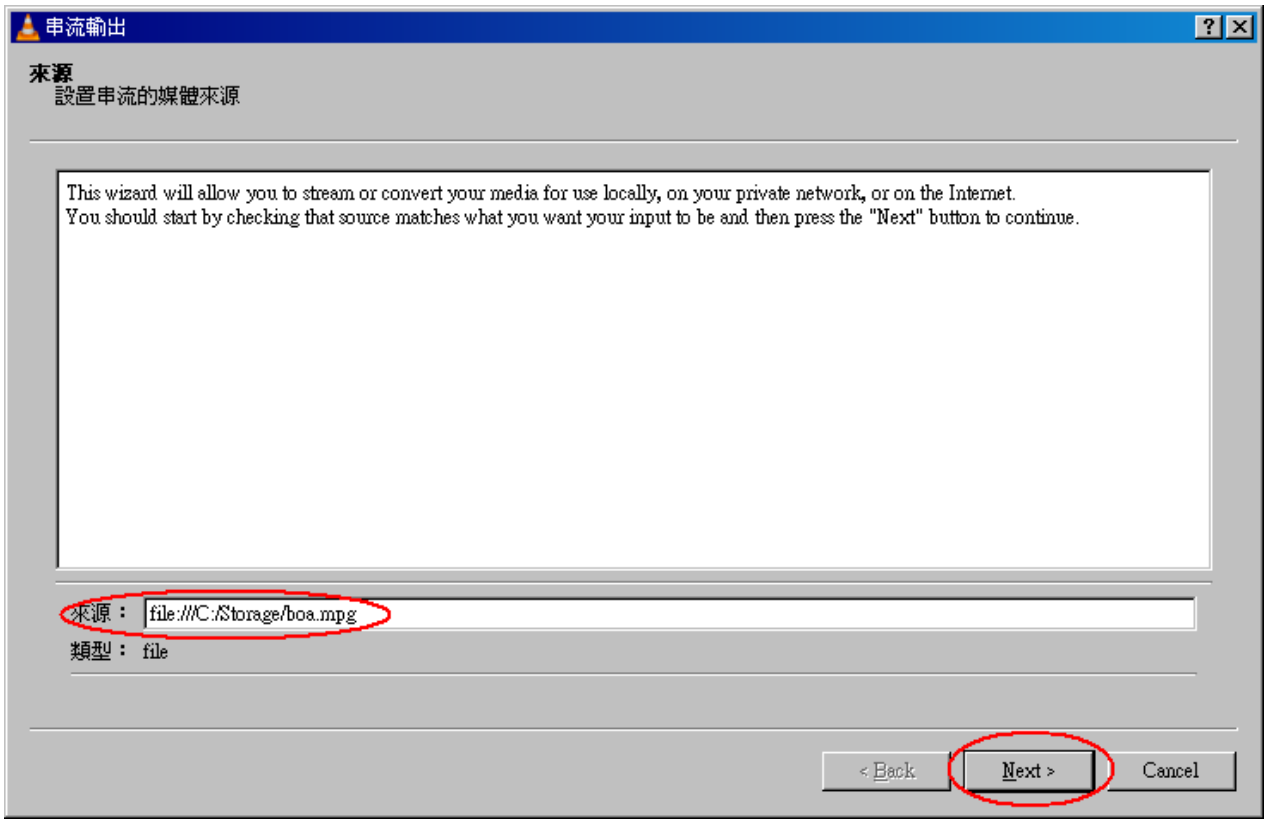
(1) In «Media » area of top tool bar to select “Stream”



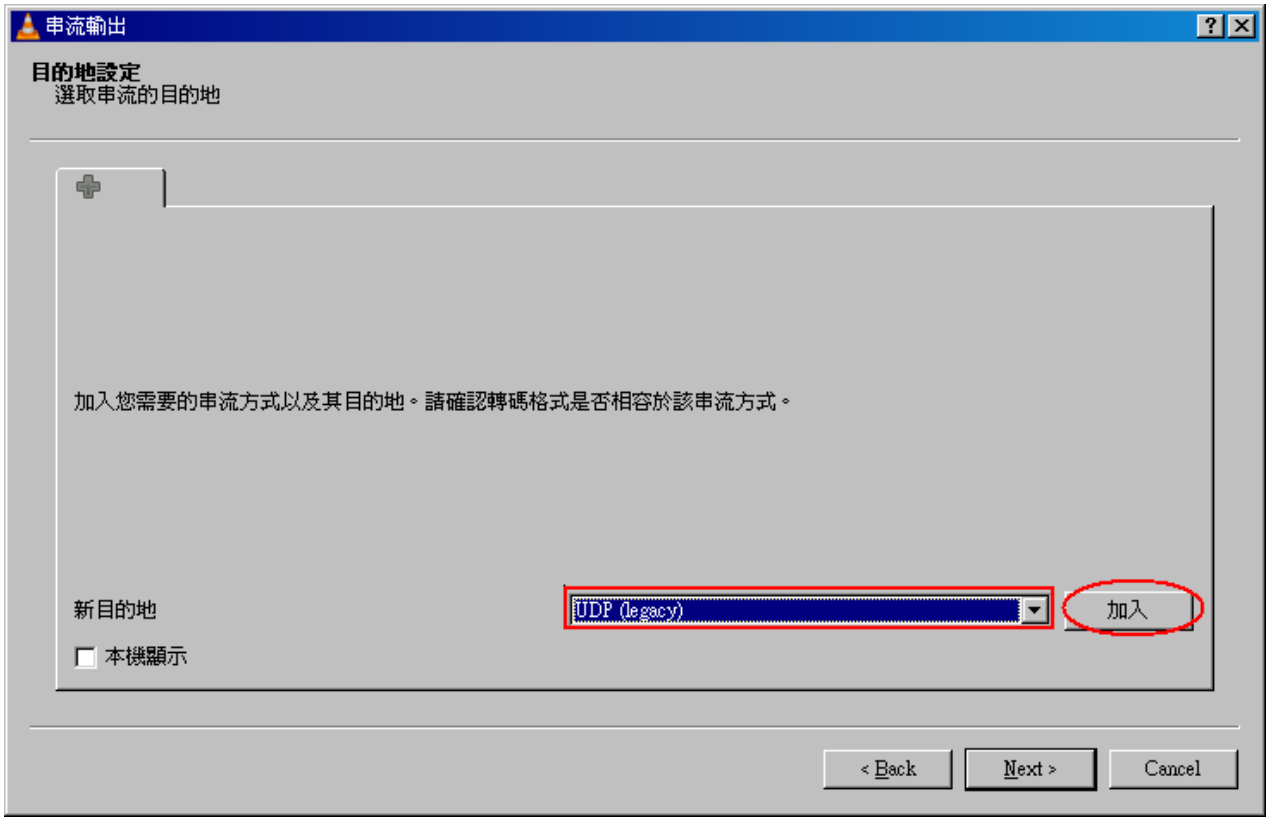
(2) Select a video or voiced file to play



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

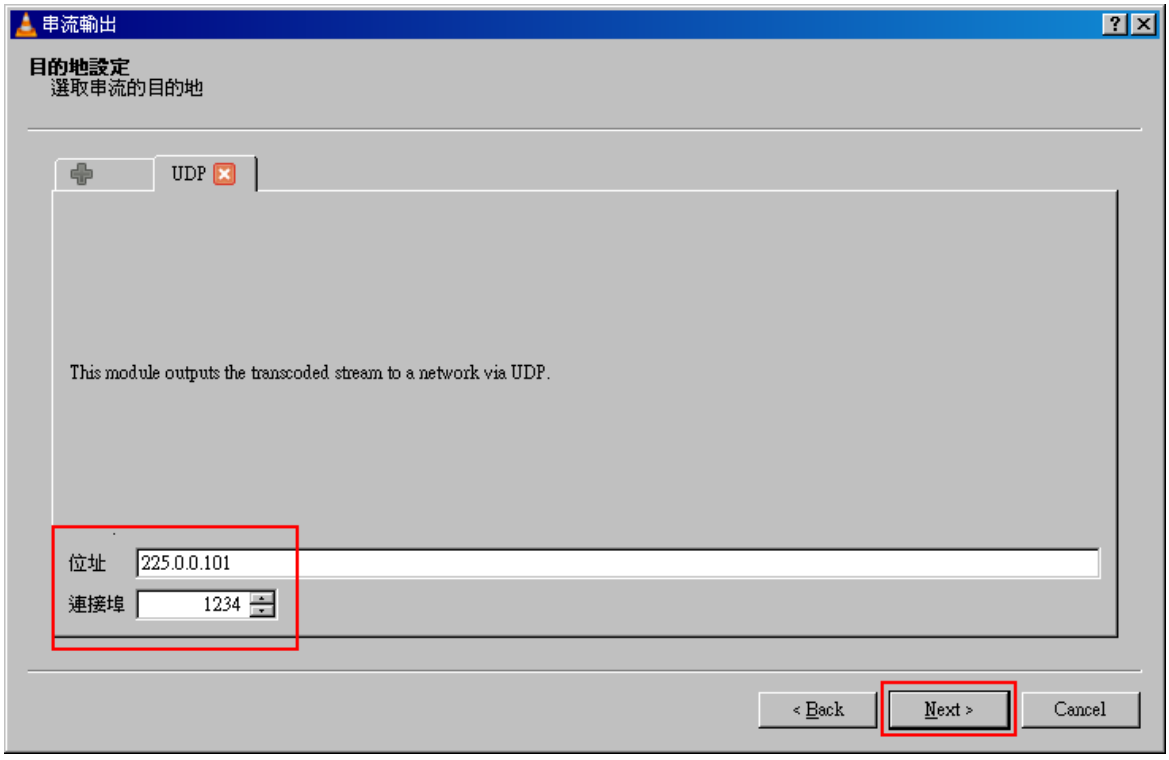


(4) Select stream type as “UDP” and click “Add” button.

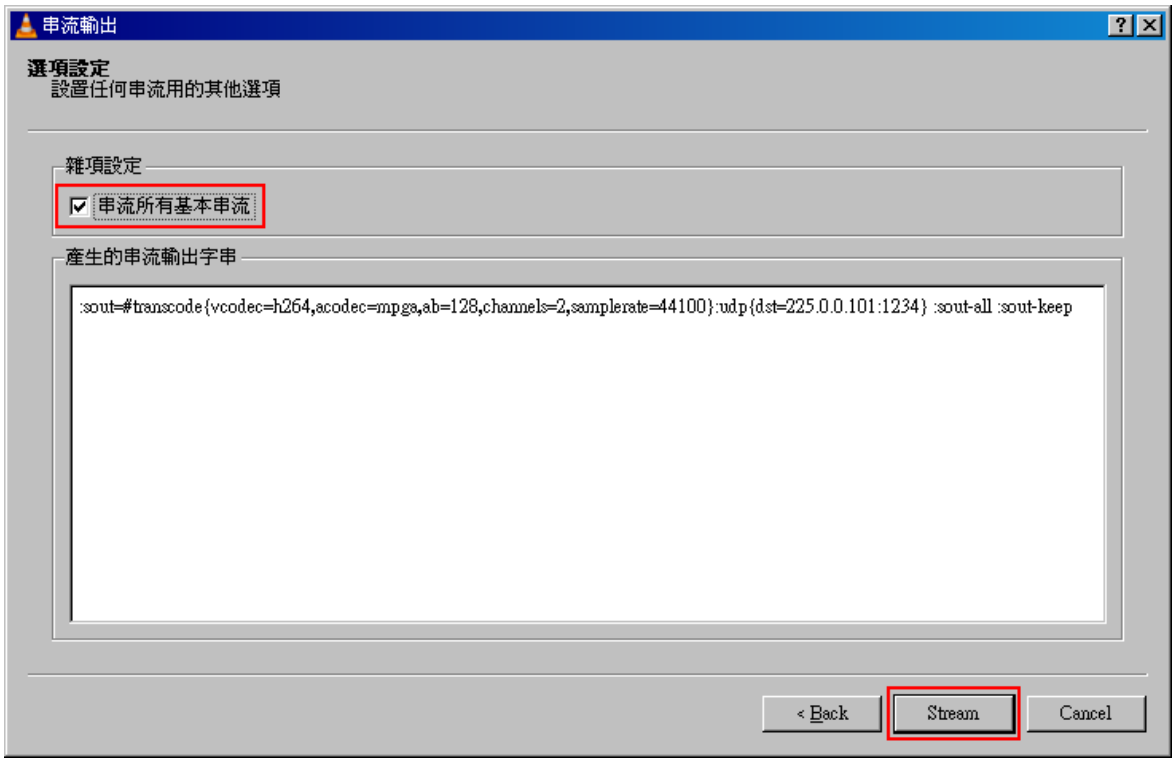


(5) Set stream IP, the range is 224.0.0.1 to 239.255.255.254, and protocol port is 1234.

Here I set stream IP is 255.0.0.1.

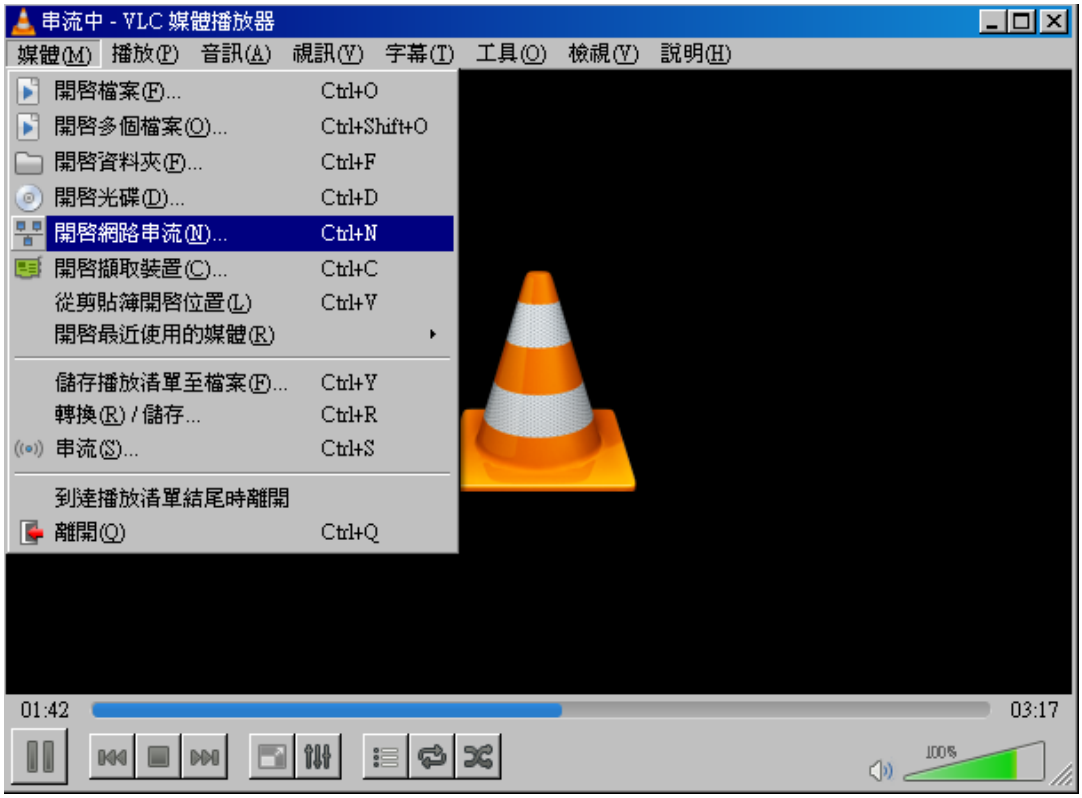


(6) Select ”Sort out all stream” and click “Stream” button, then the stream start to send to switch.



VLC Configure on IGMP Client

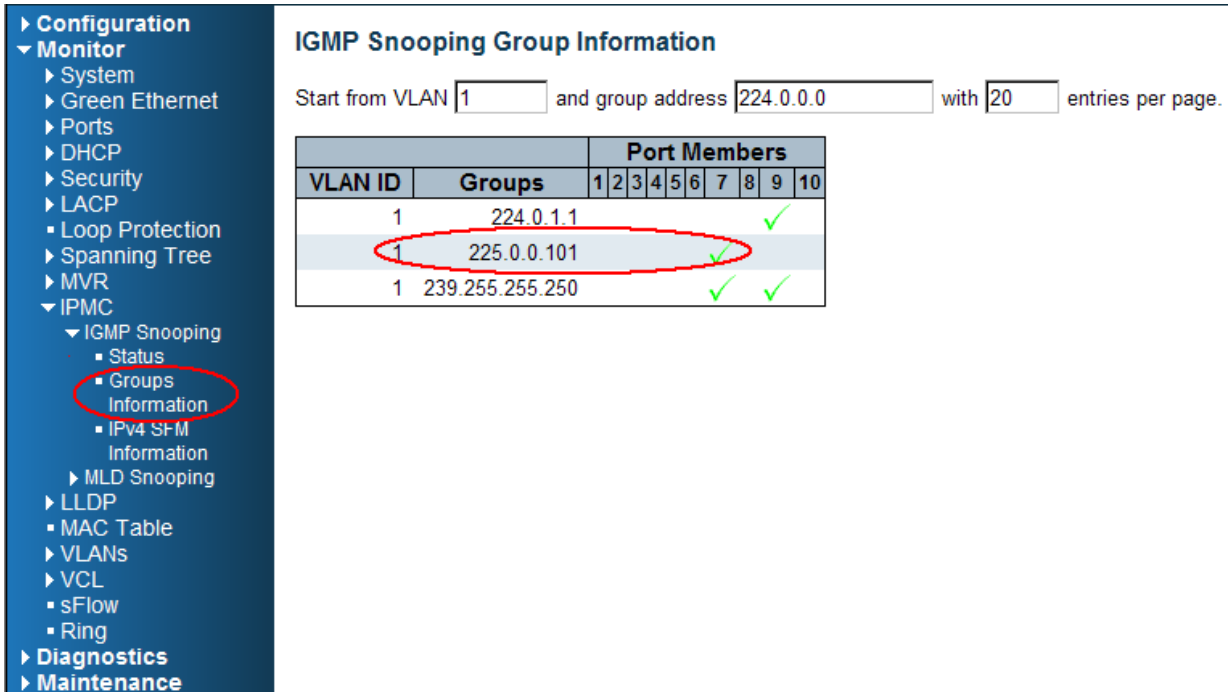
(1) In «Media » area of top tool bar to select open network stream



(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 (IPG500), 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 IPG500 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 IPG500

Item	Parameter (sec)	Description
1	ReAuth Period	IPG500 will restart authentication after each Reauth-Period when authentication success and ReAuth option is enabled
2	Quiet Period	IPG500 will wait QuietPeriod to restart authentication process again when authentication failed in previous time.
3	Tx Period	IPG500 will send EAP-request to Supplicant every TxPeriod when authentication is running and Quiet Period is not running.
4	Supplicant Timeout	IPG500 will wait SupplicantTmeout to receive response from Supplicant.
5	Server Timeout	IPG500 will wait ServerTimeout to receive response from RADIUS server.

Configuration in RADIUS Server

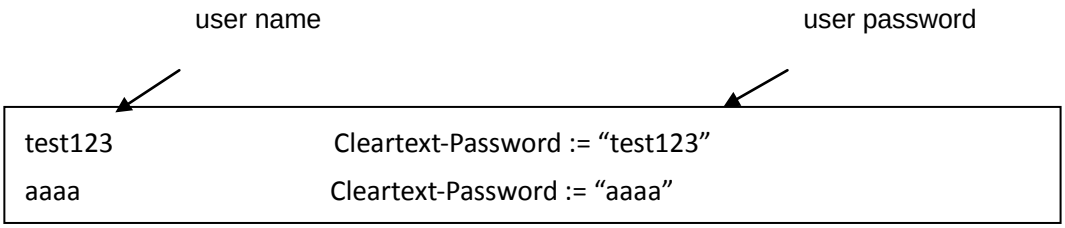
Step 1: Prepare a Linux PC with RADIUS server installed.

Step 2: Edit secret key for Radius server.

Setting:

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

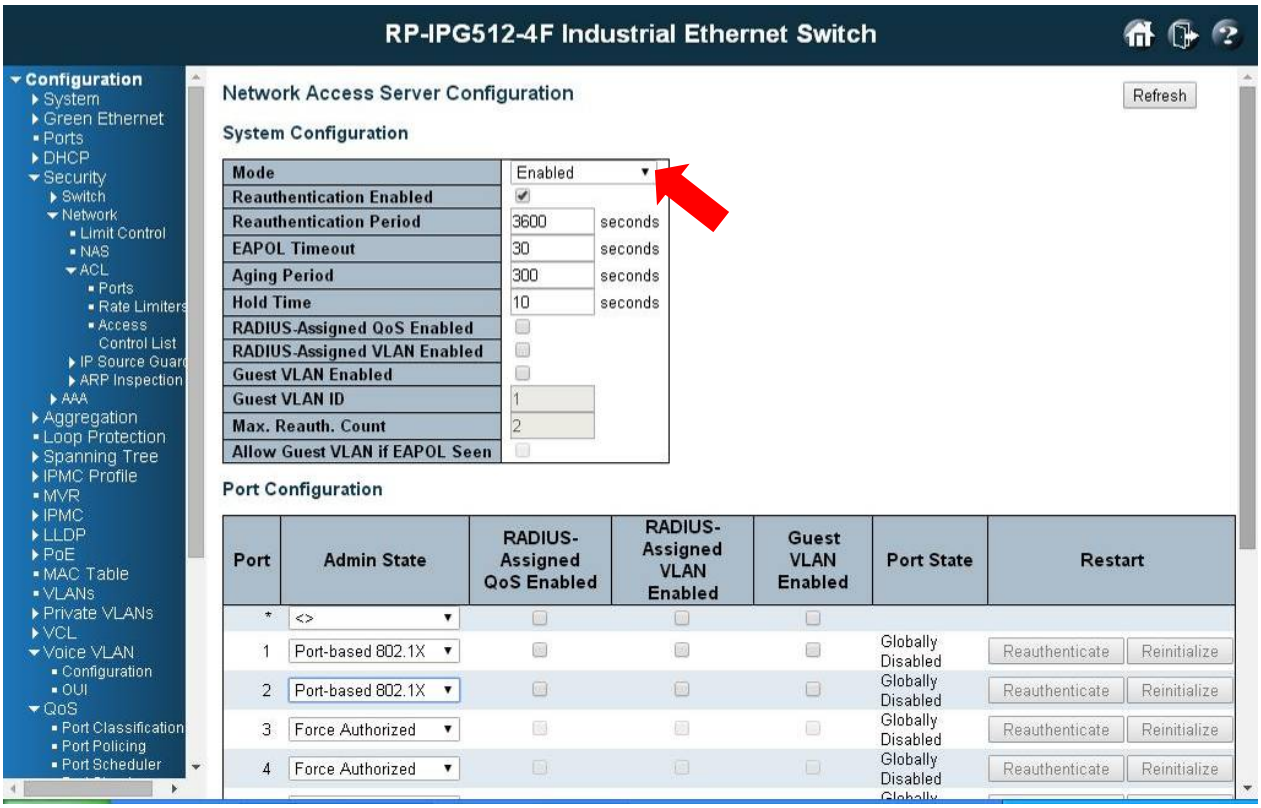
Example

Here we take an example of 802.1x Authentication via IPG500 to be authenticated by RADIUS server. In a basic example, we take port 1 as a testing port which enables 802.1x in IPG500.

With default configuration, use the following Web UI setting .

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

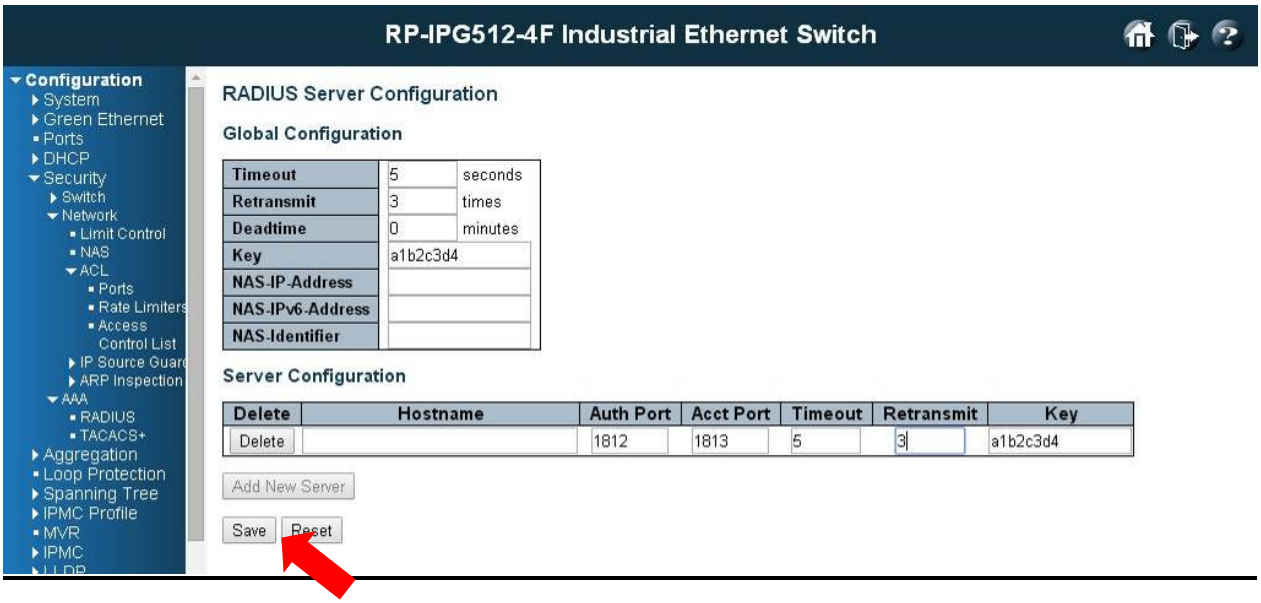
Select “Enable” mode to enable authentication, and set port-1, port-2 be “Port Base 802.1x”.



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

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

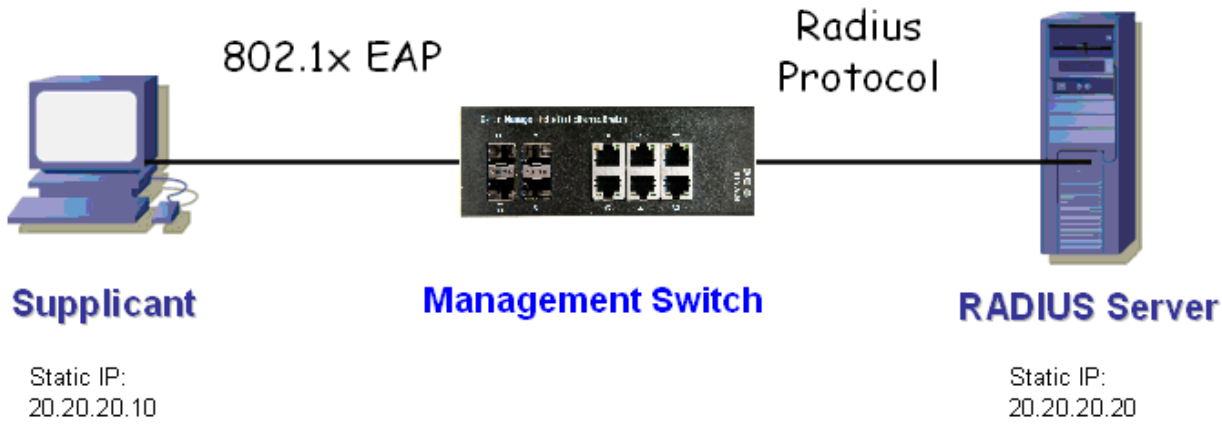
Then click “Save” button.



CLI Command:

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

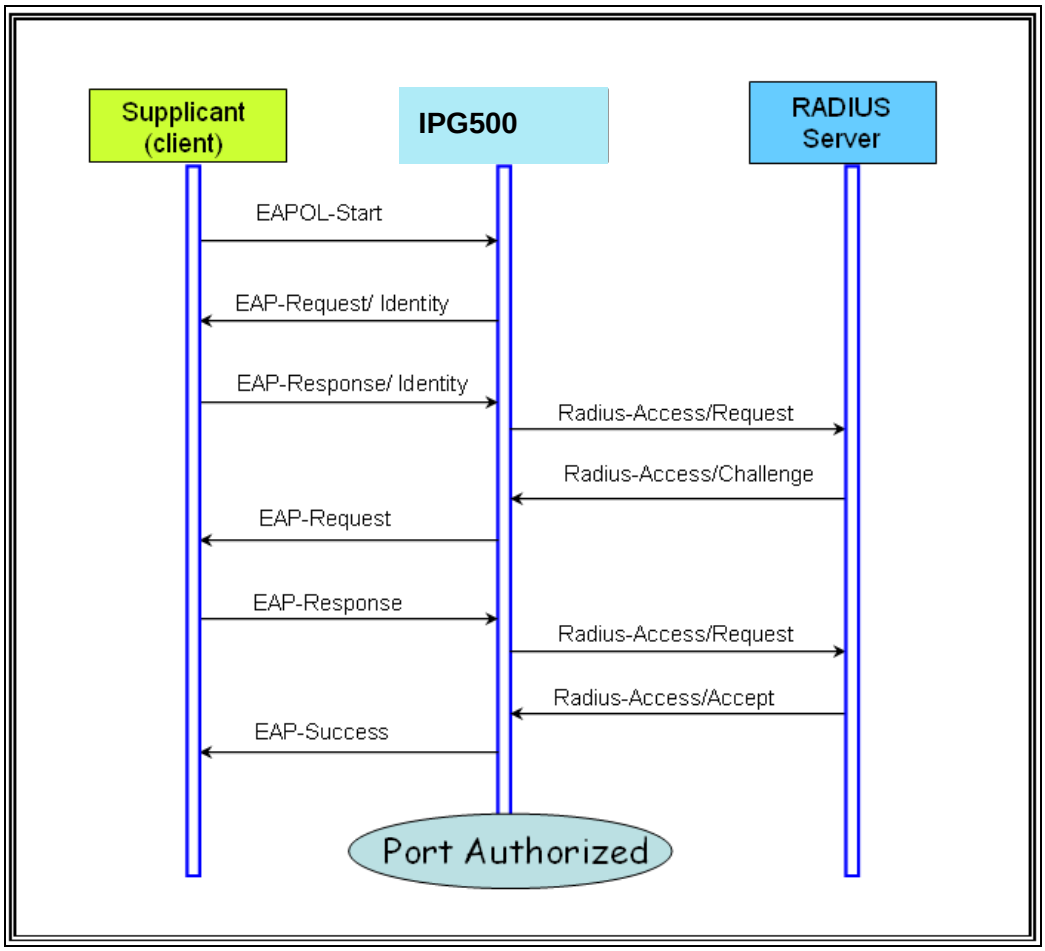
(If there is a DHCP server to assign IP address for supplicant, this step can be ignored.)

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 IPG500.

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.

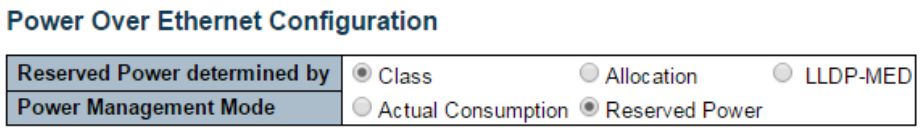


Power over Ethernet (PoE) Application Guide

IPG500 series switches support PoE function for connected powered device. The operation mode contains 802.3af (15.4W), 802.3at (30W), and 802.3at with 4 pair used (60W). 60 watt only can be applied for port 1 and 2. Each port has 5 classes for selection, class 0~4. And, total power budget of the system is up to 240 watt.

For power management friendly use, it supports power scheduler for each PoE port. Each time interval is 30 minutes from Sunday to Saturday. Customer can select which interval to set PoE on or PoE off. It also supports PoE reset function to power off, then power on the PoE function on a port at certain time. Maximum five time can be created in a week.

Reserved Power Determination



There are three modes for configuring how the ports/PDs may reserve power.

1. Class mode:

In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Five different port classes exist and one for 4, 7, 15.4 or 30 Watts.

2. Allocated mode:

In this mode the user allocates the amount of power that each port may reserve.
The allocated/reserved power for each port/PD is specified in the Maximum Power fields.

3. LLDP-MED mode:

This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly.
If no LLDP information is available for a port, the port will reserve power using the class mode

Note:
For all modes: If a port uses more power than the reserved power for the port, the port is shut down.

Power Management Mode

Power Over Ethernet Configuration

Reserved Power determined by	◉ Class	○ Allocation	○ LLDP-MED
Power Management Mode	○ Actual Consumption	◉ Reserved Power	

There are 2 modes for configuring when to shut down the ports:

1. **Actual Consumption:**

   In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down.

   Port Priority: Critical > High > Low.

   When priorities are the same, low number of the port has higher priority.

2. **Reserved Power:**

   In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply.

Other Setting Parameter

PoE Power Supply Configuration

Primary Power Supply [W]
240

PoE Port Configuration

Port	Mode	Operation	4Pairs	Priority	Maximum Power [W]
*	<>	<>	<>	<>	15.4
1	Disable	802.3af	Disable	Low	15.4
2	Disable	802.3af	Disable	Low	15.4
3	Disable	802.3af	Disable	Low	15.4
4	Disable	802.3af	Disable	Low	15.4
5	Disable	802.3af	Disable	Low	15.4
6	Disable	802.3af	Disable	Low	15.4
7	Disable	802.3af	Disable	Low	15.4
8	Disable	802.3af	Disable	Low	15.4

1. PoE Power Supply

For being able to determine the amount of power the PD may use, it must be defined what amount of power a power source can deliver. Valid values are in the range 0 to 240 Watts.

2. PoE Mode

The PoE Mode represents the PoE operating mode for the port.

Disable : PoE disabled for the port.

Enable : Enables PoE for the port.

Schedule : Enables PoE for the port by scheduling.

3. Operation Mode

The Operation Mode represents the PoE power operating protocol for the port.

802.3af : Sets PoE protocol to IEEE 802.3af.

802.3at : Sets PoE protocol to IEEE 802.3at.

4. 4 Pair

The 4Pairs represents the 60W power supply for the port.

The option is only available when following rules are applied.

- High power switch model supports.
- Only port1 or port2 supports.
- Current operation mode is 802.3at.

Enable : Enable 4Pairs to support 60W.

Disable : Disable 4Pairs to limit 30W of power.

5. PoE Priority

The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical.

The priority is used in the case where the remote devices require more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.

6. Maximum Power

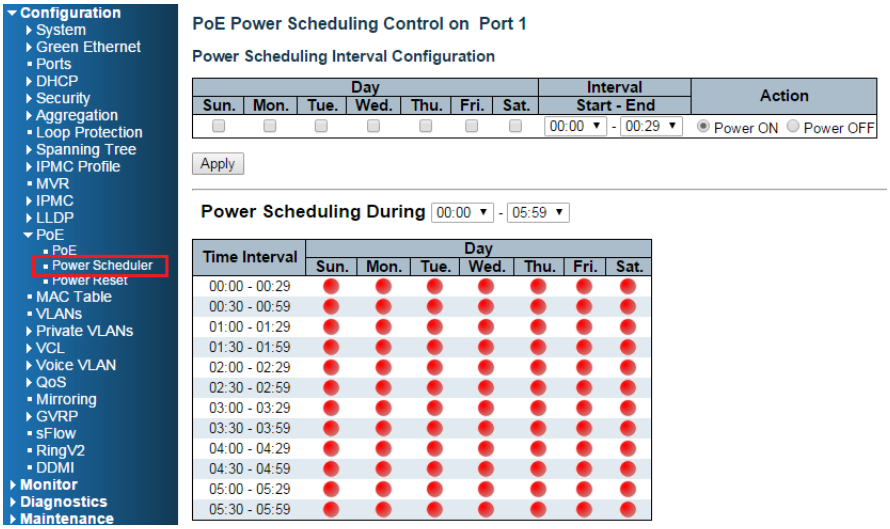
The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device.

For port support 4Pairs mode, the maximum allowed value is 60 W; others are 30 W.

PoE Power Scheduling & Reset

The power scheduling is used to control the power alive interval on PoE port. It is allowed to set the specific interval to schedule power on/off in one week.

The current scheduling state is displayed graphically during the week. Green indicates the power is on and red that it is off. Directly changes checkmarks to indicate which day are members of the time interval. Check or uncheck as needed to modify the scheduling table.



1. **Day**

   Checkmarks indicate which day are members of the set. From Sunday to Saturday.

2. **Interval**

   Start - Select the start hour and minute. End - Select the end hour and minute.

   There are 48 time interval one day. Each interval has 30 minutes.

3. **Action**

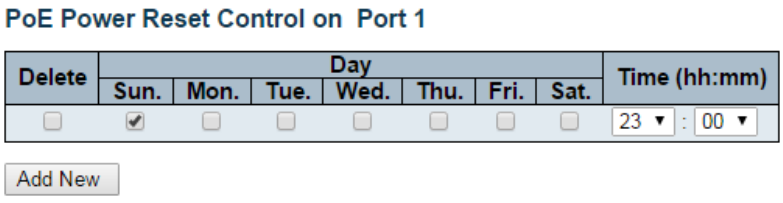
   Power On - Select the radio button to apply power on during the interval.

   Power Off - Select the radio button to apply power off during the interval.

4. **PoE Power Reset**

   The entry is used to control the power reset time on PoE port.

   It is allowed to create at maximum 5 entries for each PoE port.



Example 1

1. **Parameter Setting:**

   Reserved Power determined: Class

   Power Management Mode: Actual Consumption

   Primary Power Supply: 6W

2. **Test Port**

   Port 1: 802.3at with critical priority

   Port 2: 802.3af with high priority

   Port 3: 802.3af with low priority

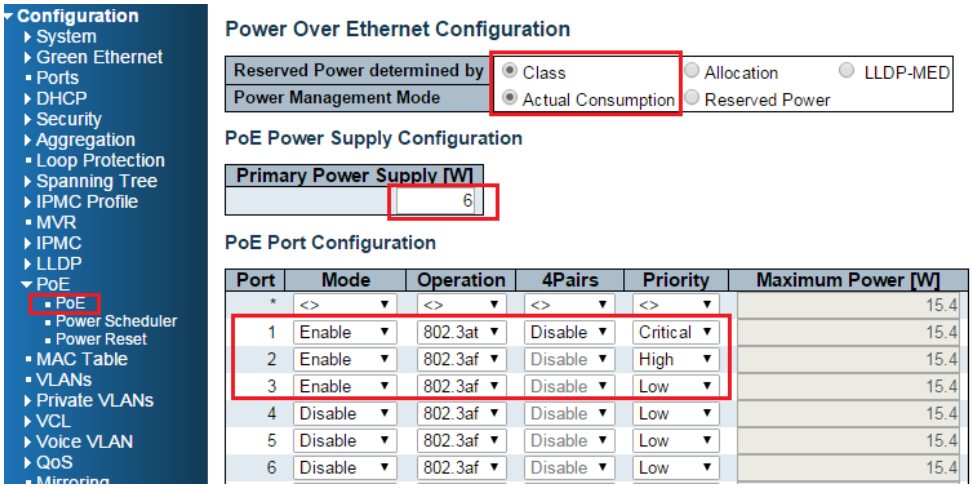
3. **PD Power Consumption**

   Port 1: 1.3 watt (PoE Splitter)

   Port 2: 1.3 watt (PoE VoIP Phone)

   Port 3: 3.8 watt (PoE WiFi AP)

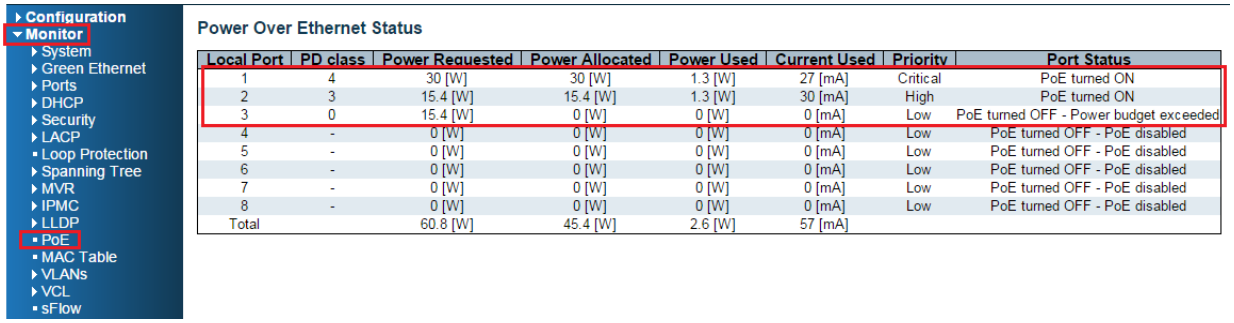
4. **Web Configuration**



5. **Test Result**

   PoE port status can be monitored by Web: Monitor→PoE

   In the following table, it can be seen if system budget is not enough for all PoE device, port with higher priority port will be feed power first. The last priority port (port 3) will not be powered.



Example 2

1. Parameter Setting:

Reserved Power determined: Allocation

Power Management Mode: Reserved Power

Primary Power Supply: 138 W (> all port reserved power)

2. Port Maximum Power

Port 1: 30 W

Port 2~ Port8: 15.4 W

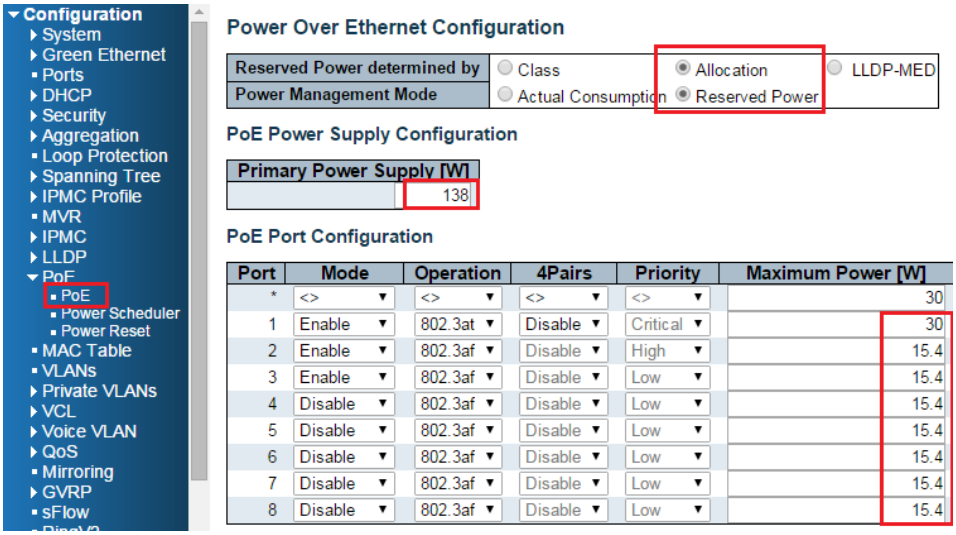
Total: 137.8 W

3. PD Power Consumption

Port 1: 1.3 watt (PoE Splitter) Port 2: 1.3 watt (PoE VoIP Phone)

Port 3: 3.8 watt (PoE WiFi AP)

4. Web Configuration



5. Test Result

PoE port status can be monitored by Web: Monitor→PoE

Since power has reserved for each port in advance, each powered device can use power budget of its corresponding port without exceed its maximum power.