MRI-128-F4G Series

User's Manual

Version 1.2

Industrial Managed

Ethernet Switch

www.westermo.com

Copyright Notice

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his expense.

The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user’s authority to operate this equipment.

Index

1 Introduction

Welcome to MRI-128-F4G Rackmount Managed Ethernet Switch User Manual.
Following topics are covered in this chapter:

1.1 Overview

1.2 Major Features

1.3 Package Checklist

1.1 Overview

The MRI-128-F4G Series, the 19-inch 24+4G Managed Ethernet Ring Switch, is equipped with 24 10/100 Base-TX ports plus 4 Gigabit RJ45 / MINI GBIC combo ports. The switch is specially designed for control rooms where high-port density and performance are required. The Gigabit Combo port allows 10/100/1000 triple speed of copper ports, and the SFP ports accept all types of Gigabit SFP transceivers, including Gigabit SX, LX, LHX, ZX and XD for several connections and distances.

Model Name	Description
MRI-128-F4G	Rackmount Managed Ethernet Switch with 24 10/100Base-TX + 4 Gigabit Combo Ports, 90-264VAC input
MRI-128-F4G/DC	Rackmount Managed Ethernet Switch with 24 10/100Base-TX + 4 Gigabit Combo Ports, 24V (12-48V) DC input

The device is mounted within the 19 inch rack, along with other 19 inch public servers or other network devices. When other industrial switches are aggregated to the switch, the 24+4G design allows connecting up to 12 100M rings plus 2 Gigabit rings and each ring has its own ring redundancy protection.

The switch is designed as a fan-less rackmount switch with low power consumption and wide operating temperature. The MRI-128-F4G/DC allows 24V (12-48V) DC input. The switch supports Jumbo frame featuring up to 9,216 bytes packet size for large size file transmission which is the trend for future industrial application requests.

The switch supports RSTP, Multiple Super Ring technology, VLAN, IGMP

Snooping, LACP for network control, SNMP and LLDP for network management. Secured access is protected by Port Security, 802.1x and flexible Layer 2/4 Access Control List.

1.2 Major Features

- 24-port 10/100 Base-TX and 4-port Gigabit RJ-45/SFP combo ports (10/100/1000 Base-TX, 1000Base-X)
- Non-Blocking Switching Performance, no collision or delay when wire-speed transmission
- Supports Jumbo Frame up to 9,216 byte
- IEEE 802.1s MSTP, RSTP and Multiple Super Ring (Rapid Super Ring, Rapid Dual Homing, MultiRing, TrunkRing)
- Maximum 12 x 100M Rings plus 2 Gigabit Rings aggregation capability
- VLAN, LACP, GVRP, QoS, IGMP Snooping, Rate Control, Online Multi Port Mirroring and WeDashboard
- Link Layer Discovery Protocol (LLDP), SNMP V1/V2c/V3, RMON
- Advanced Security supports IP/Port Security, DHCP Server, 802.1x and Access Control List
- Supports Modbus TCP/IP for Factory Automation
- Event Notification by E-mail, SNMP Trap, Syslog and Relay Output
- 90-264VAC or Dual 12-48VDC power input

1.3 Package List

MRI-128-F4G 24+4G Rackmount Managed Ethernet Ring Switch

Includes:

- The switch (no SFP transceivers)
- Rack Mount Kit
- Console Cable
- Power Cord
- Document CD

MRI-128-F4G/DC 24+4G Rackmount Managed Ethernet Ring Switch with 12-48VDC input

Includes:

- The switch (no SFP transceivers)
- Rack Mount Kit

- Console Cable
- Document CD

If any of the above items are missing or damaged, please contact your local sales representative.

2 Hardware Installation

This chapter includes hardware introduction, installation and configuration information.
Following topics are covered in this chapter:

2.1 Hardware Introduction

LED

System: Power (Green), Ring Master (Green)

10/100 RJ-45:

Link/Activity: Green = 100M, Yellow = 10M;

Duplex: On = Full, Off = Half

Gigabit Copper/SFP:

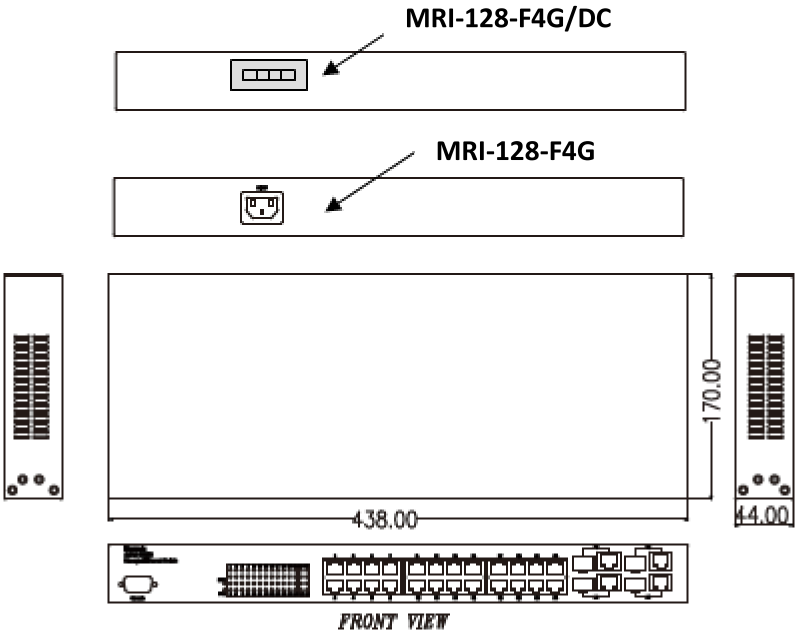
Link/Activity: Green = 1000M, Yellow = 10M or 100M;

Duplex: On = Full, Off = Half)

Gigabit SFP: Link/Activity (Green/Green Blinking)

Dimension

44mm(H) x 438mm (W) x 170mm (D)



Panel Layout

The front panel includes RS-232 Console Port, System & Port LEDs, Fast Ethernet Port Interfaces and Gigabit Combo Port Interfaces.

The console port chooses RS-232 DB-9 types. The pin arrangement is “Pin2: TxD, Pin3: RxD, Pin5: GND”. The console cable is shipped with the switch.

In the Rear panel, there are 2 types power input connector applied to the switch and the switch-DC.

The AC variant uses standard AC plug as power input socket. The DC variant uses 4-pin terminal block as power input socket. Follow the V+, V- indication in the rear panel to screw the power source.

2.2 Wiring Power Inputs

The MRI-128-F4G series provides two variances with different power inputs.

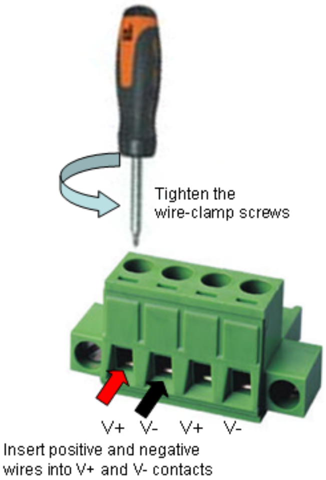
AC Power Input

Connect the attached power cord to the AC power input connector, the available AC power input is range from 90-264VAC.

DC Power Input

The suggested power input is 24VDC, the available range is from 12-48VDC.

Follow below steps to wire the switch redundant DC power inputs.


Tighten the wire-clamp screws
V+ V- V+ V-
Insert positive and negative wires into V+ and V- contacts

1. Insert positive and negative wires into V+ and V- contacts respectively of the terminal block connector
2. Tighten the wire-clamp screws to prevent DC wires from being loosened.
3. Power 1 and Power 2 support power redundancy.
4. Positive and negative power system inputs are both accepted, but Power 1 and Power 2 must apply the same mode.

Note 1: It is a good practice to turn off input and load power, and to unplug power terminal block before making wire connections. Otherwise, your screwdriver blade can inadvertently short your terminal connections to the grounded enclosure.

Note 2: The range of the suitable DC electric wire is from 12 to 24 AWG.

Note 3: Please follow the V+ and V- indicator. Incorrect wiring would not damage the switch; only prevent the switch to power up

Note 4: Please follow the V+ and V- indicator. Incorrect wiring would not damage the switch, only prevent the switch to power up

2.3 Wiring Earth Ground

To ensure the system will not be damaged by noise or any electrical shock, we suggest you to make exact connection with Earth Ground.

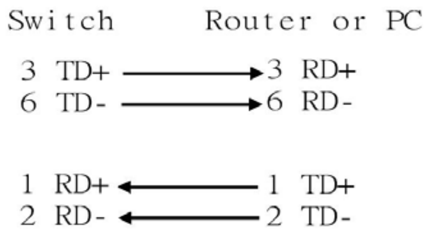
For AC input, the 3 pin include V+, V- and GND. The GND pin must be connected to the earth ground.

For DC input, loosen the earth ground screw using a screw driver; then tighten the screw after earth ground wire is connected.

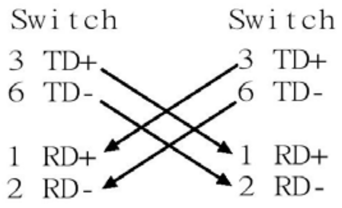
2.4 Wiring Fast Ethernet Ports

The switch includes 24 RJ-45 Fast Ethernet ports. The Fast Ethernet ports support 10Base-T and 100Base-TX, full or half duplex modes. All the Fast Ethernet ports will auto-detect the signal from connected devices to negotiate the link speed and duplex mode. Auto MDI/MDIX allows users to connect another switch, hub or workstation without changing straight through or crossover cables.

Note that crossover cables simply cross-connect the transmit lines at each end to the received lines at the opposite end.



Straight-through Cabling Schematic



Cross-over Cabling Schematic

Note that Ethernet cables use pins 1, 2, 3, and 6 of an 8-pin RJ-45 connector. The signals of these pins are converted by the automatic MDI-X function, as shown in the table below:

Pin MDI-X	Signals	MDI Signals
1	RD+	TD+
2	RD-	TD-
3	TD+	RD+
6	TD-	RD-

Connect one side of an Ethernet cable into any switch port and connect the other side to your attached device. The LNK LED will light up when the cable is correctly connected. Refer to the **LED Indicators** section for descriptions of each LED indicator. Always make sure that the cables between the switches and attached devices (e.g. switch, hub, or workstation) are less than 100 meters (328 feet).

The wiring cable types are as below.

10Base-T: 2-pair UTP/STP Cat. 3, 4, 5 cable, EIA/TIA-568 100-ohm (100m)

100 Base-TX: 2-pair UTP/STP Cat. 5 cable, EIA/TIA-568 100-ohm (100m)

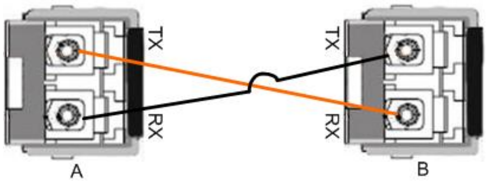
1000 Base-TX: 4-pair UTP/STP Cat. 5e cable, EIA/TIA-568 100-ohm (100m)

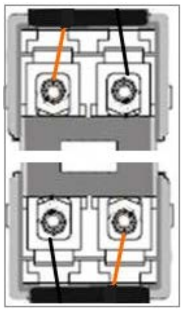
2.5 Wiring Fiber Ports

Small Form-factor Pluggable (SFP)

The SFP ports fulfill the SFP standard. To ensure the system reliability, it is recommended to use the approved Gigabit SFP Transceiver. The web user interface will show Unknown vendor type when choosing the SFP which is not approved.

The way to connect the SFP transceiver is to Plug in SFP fiber transceiver first. Cross-connect the transmit channel at each end to the receive channel at the opposite end as illustrated in the figure below.





Note: This is a Class 1 Laser/LED product. Don't look into the Laser/LED Beam.

2.6 Wiring Gigabit Combo Ports

The switch includes 4 RJ-45 Gigabit Ethernet ports which supports 10Base-T, 100Base-TX and 1000Base-TX. The switch is also equipped with 4 Gigabit SFP ports combo which supports 1000Base-SX/LX and is according the standard MINI GBIC SFP transceiver.

While the SFP transceiver is plugged, the Fiber port has higher priority than copper port and moved to the Fiber mode automatically.

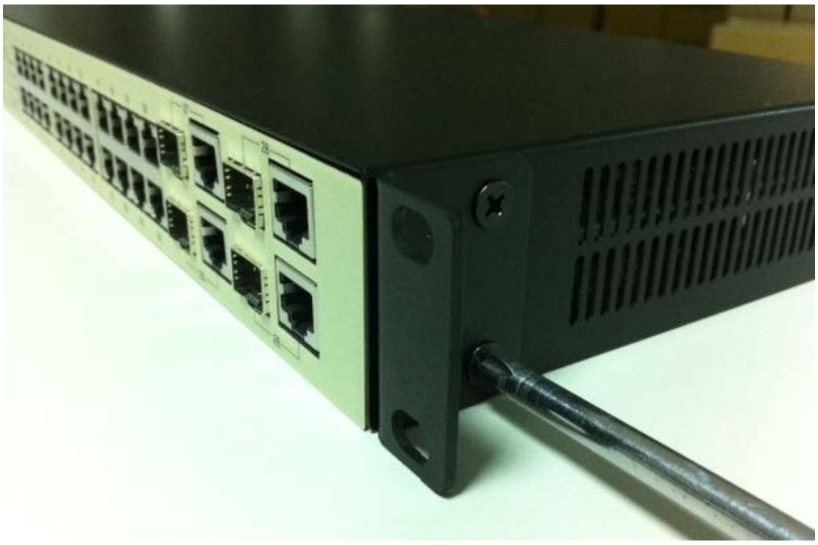
2.7 Wiring RS-232 Console Cable

Westermo attaches one RS-232 DB-9 to DB-9 cable in the box. Connect the DB-9 connector to the COM port of your PC, open Terminal tool and set up serial settings to 9600, N,8,1. (Baud Rate: 9600 / Parity: None / Data Bit: 8 / Stop Bit: 1) Then you can access the CLI interface using the console cable.

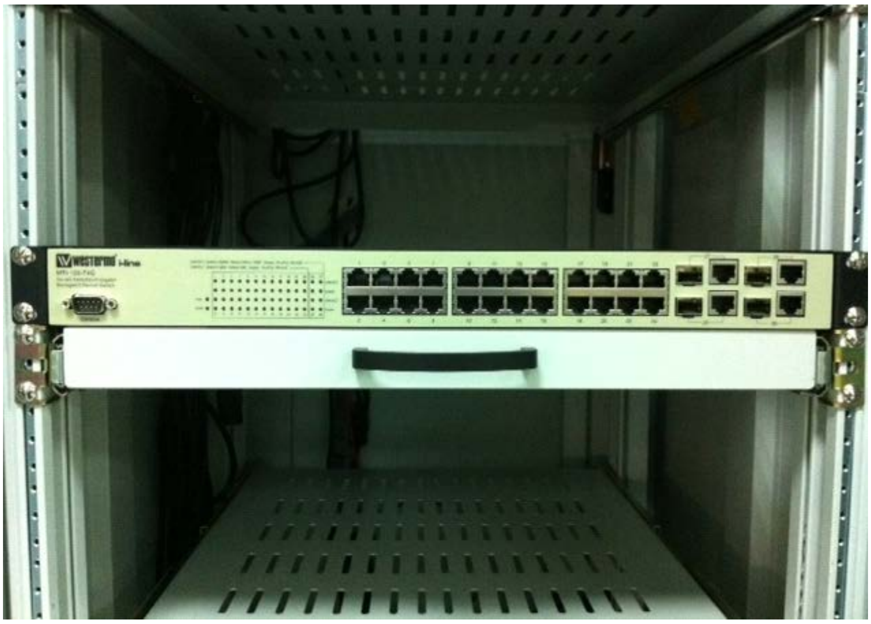
Note: If you lost the cable, please contact your local sales office or follow the pin assignment to buy/make a new one. The pin assignment spec is listed in the appendix.

2.8 Rack Mounting Installation

The Rack Mount Kit is attached inside the package box.



Attach the brackets to the device by using the screws provided in the Rack Mount kit.



Mount the device in the 19’ rack by using four rack-mounting screws.

When installing multiple switches, mount them in the rack one below the other. It’s requested to **reserve 0.5U-1U free space for multiple switches installing in high temperature environment.** This is important to disperse the heat generated by the switch.

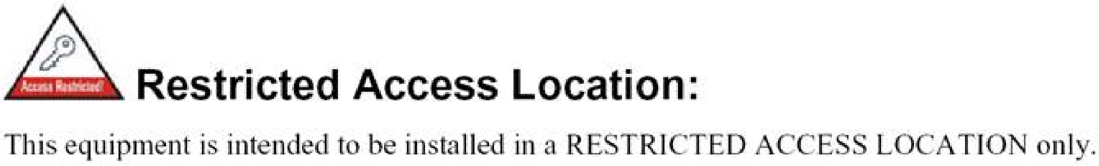
Notice when installing:

- Temperature: Check if the temperature conforms to the specified operating temperature range.

- Mechanical Loading: Do no place any equipment on top of the switch. In high vibration environment, additional rack mounting protection is necessary, like the flat board under/above the switch.
- Grounding: Rack-mounted equipment should be properly grounded.

2.9 Safety Warning

2.2.1 The Equipment intended for installation in a Restricted Access Location.


Access Restricted!

Restricted Access Location:

This equipment is intended to be installed in a RESTRICTED ACCESS LOCATION only.

2.2.2 The warning test is provided in user manual. Below is the information:
”For tilslutning af de ovrige ledere, se medfolgende installationsvejledning”.
“Laite on liitettava suojamaadoitus-koskettimilla varustettuun pistorasiaan”
“Apparatet ma tilkoples jordet stikkontakt“
”Apparaten skall anslutas till jordat uttag”

3 Preparation for Management

The switch provides both in-band and out-band configuration methods. You can configure the switch via RS232 console cable if you don't attach your admin PC to your network, or if you lose network connection to the switch. This is so-called out-band management. It wouldn't be affected by network connectivity.

The in-band management means you can remotely manage the switch via the network. You can choose Telnet or Web-based management. You just need to know the device's IP address and you can remotely connect to its embedded HTTP web pages or Telnet console.

Following topics are covered in this chapter:

3.1 Preparation for Serial Console

3.2 Preparation for Web Interface

3.3 Preparation for Telnet console

3.1 Preparation for Serial Console

In the package, there is one RS-232 DB-9 to DB-9 console cable. Please attach RS-232 DB-9 connector to your PC COM port, connect the other end to the Console port of the switch. If you lose/lost the cable, please follow the console cable PIN assignment to find a new one, or contact your closest Westermo sales office. (Refer to the appendix).

1. Go to Start -> Program -> Accessories -> Communication -> Hyper Terminal
2. Give a name to the new console connection.
3. Choose the COM name
4. Select correct serial settings. The serial settings of the switch are as below:
   Baud Rate: 9600 / Parity: None / Data Bit: 8 / Stop Bit: 1
5. After connected, you can see Switch login request.
6. Log into the switch. The default username is "admin", password, "westermo".

```
Switch login: admin
Password:

The switch (version 1.1-20101014-11:04:13).

Switch>
```

3.2 Preparation for Web Interface

The switch provides HTTP Web Interface and Secured HTTPS Web Interface for web management.

3.2.1 Web Interface

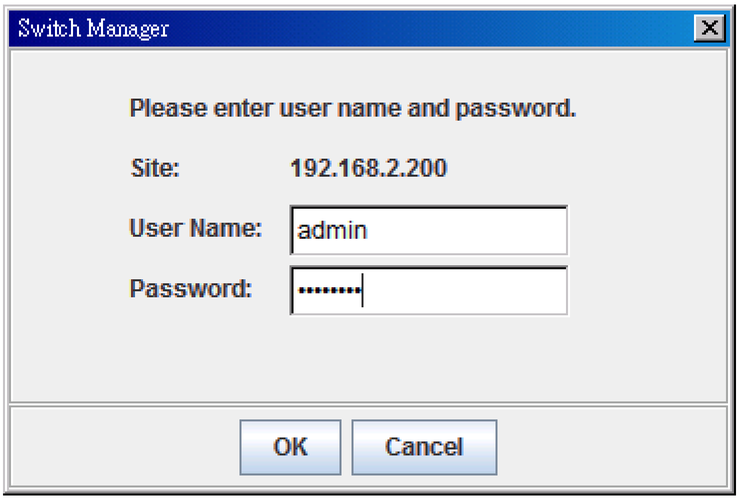
Web management page is developed by JAVA. It allows you to use a standard web-browser such as Microsoft Internet Explorer, or Mozilla Firefox, to configure and/or log from the switch from anywhere on the network.

Before you attempt to use the embedded web interface to manage switch operation, verify that the switch is properly installed on your network and that the PC on this network can access the switch via the web browser.

1. Verify that your network interface card (NIC) is operational, and that your operating system supports TCP/IP protocol.
2. Wire DC power to the switch and connect your switch to your computer.
3. Make sure that the switch default IP address is 192.168.2.200.
4. Change your computer IP address to 192.168.2.2 or other IP address which is located in the 192.168.2.x (Network Mask: 255.255.255.0) subnet.
5. Switch to DOS command mode and ping 192.168.2.200 to verify a normal response time.

Launch the web browser and Login.

6. Launch the web browser (Internet Explorer or Mozilla Firefox) on the PC.
7. Type **http://192.168.2.200** (or the IP address of the switch). And then press **Enter**.
8. The login screen will appear next.
9. Type in the user name and the password. Default user name is **admin** and password **westermo**.



Switch Manager

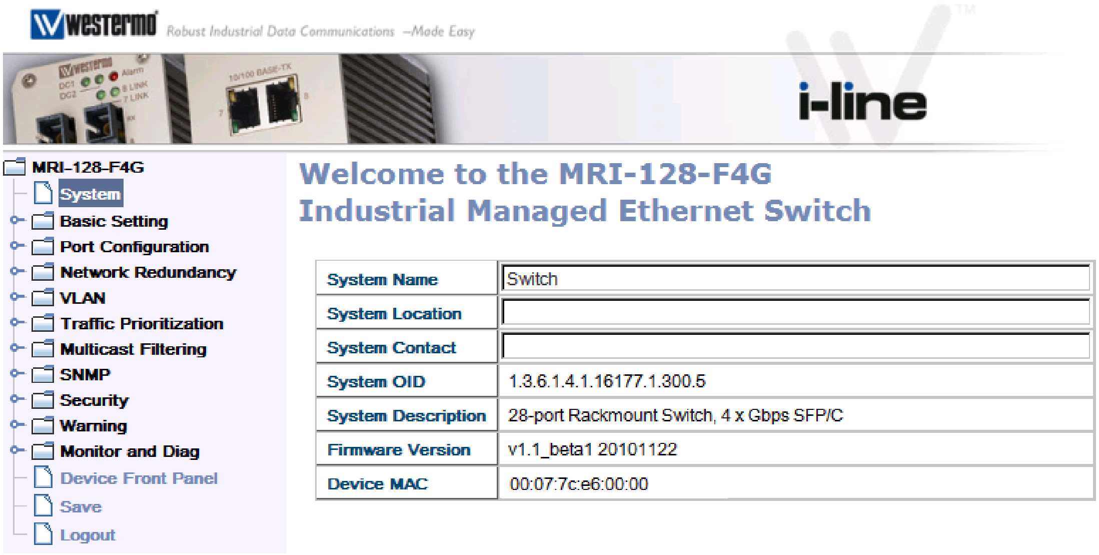
Please enter user name and password.

Site: 192.168.2.200

User Name: admin

Password: ••••••••

Click on **Enter** or **OK**. The welcome page of the web-based management interface will then appear.



Welcome to the MRI-128-F4G
Industrial Managed Ethernet Switch

System Name	Switch
System Location	
System Contact	
System OID	1.3.6.1.4.1.16177.1.300.5
System Description	28-port Rackmount Switch, 4 x Gbps SFP/C
Firmware Version	v1.1_beta1 20101122
Device MAC	00:07:7c:e6:00:00

Once you enter the web-based management interface, you can freely change the IP address to fit your network environment.

Note 1: Internet Explorer 5.0 or later versions do not allow Java applets to open sockets by default. Users have to directly modify the browser settings to selectively enable Java applets to use network ports.

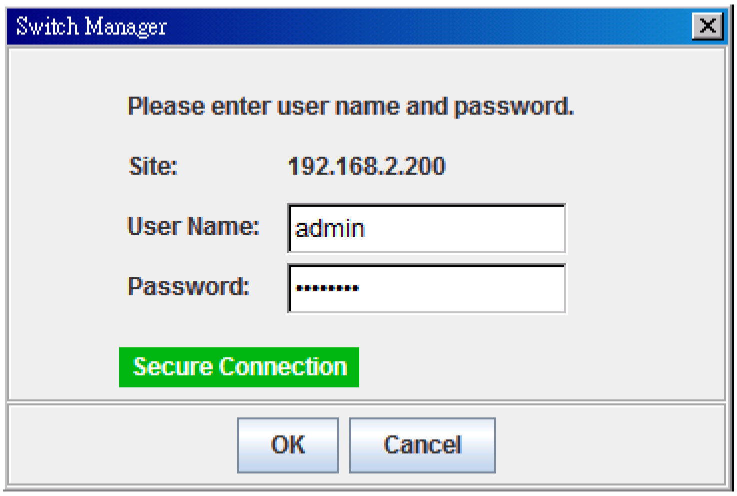
Note 2: The Web UI connection session of the switch will be logged out automatically if you don’t give any input after 30 seconds. After logged out, you should re-login and type in the correct user name and password again.

3.2.2 Secured Web Interface

Westermo web management page also provides secured management HTTPS login. All the configuration commands will be secured.

Launch the web browser and Login.

1. Launch the web browser (Internet Explorer or Mozilla Firefox) on the PC.
2. Type **https://192.168.2.200** (or the IP address of the switch). And then press **Enter**.
3. The popup screen will appear and request you to trust the secured HTTPS connection. Press **Yes** to trust it.
4. The login screen will appear next.



Please enter user name and password.

Site: 192.168.2.200

User Name: admin

Password: ••••••••

5. Key in the user name and the password. The default user name is **admin** and password is **westermo**.
6. Press **Enter** or click on **OK.** The welcome page of the web-based management interface will then appear.
7. Once you enter the web-based management interface, all the commands you see are the same as what you see by HTTP login.

3.3 Preparation for Telnet Console

3.3.1 Telnet

The switch supports Telnet console. You can connect to the switch by Telnet and the command lines are the same as what you see by RS232 console port. Below are the steps to open Telnet connection to the switch.

1. Go to Start -> Run -> cmd. And then press **Enter**
2. Type the **telnet 192.168.2.200** (or the IP address of the switch). And then press **Enter**

3.3.2 SSH (Secure Shell)

The switch also support SSH console. You can remotely connect to the switch by command line interface. The SSH connection can secure all the configuration commands you send to the switch.

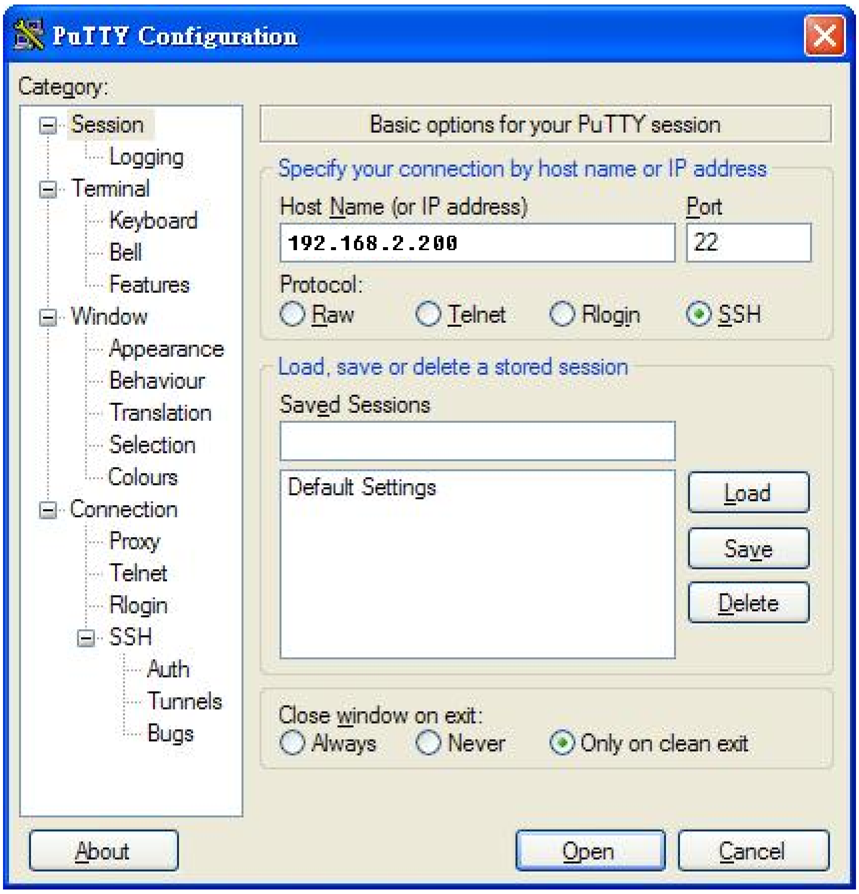
When you wish to establish a SSH connection with the switch, you should download the SSH client tool first.

SSH Client

There are many free, sharewares, trials or charged SSH clients you can find on the internet. Fox example, PuTTY is a free and popular Telnet/SSH client. We'll use this tool to demonstrate how to login SSH.

Open SSH Client/PuTTY

In the **Session** configuration, enter the **Host Name** (IP Address of the switch) and **Port number** (default = 22). Choose the "**SSH**" protocol. Then click on "**Open**" to start the SSH session console.



PuTTY Configuration

Basic options for your PuTTY session

Specify your connection by host name or IP address

Host Name (or IP address): 192.168.2.200

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

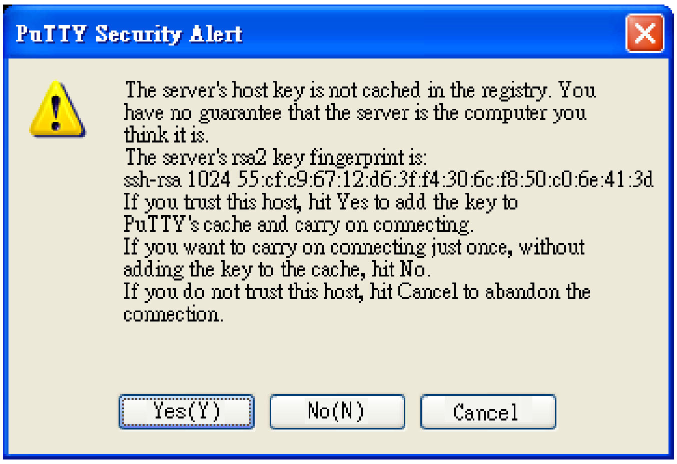
Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

After click on **Open**, then you can see the cipher information in the popup screen. Press **Yes** to accept the Security Alert.



PuTTY Security Alert

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1024 55:cf:c9:67:12:d6:3f:f4:30:6c:f8:50:c0:6e:41:3d
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

After few seconds, the SSH connection to the switch is opened.

Type the Login Name and its Password. The default Login Name and Password are **admin / westermo**.

All the commands you see in SSH are the same as the CLI commands you see via RS232 console. The next chapter will introduce in detail how to use command line to configure the switch.

4 Feature Configuration

This chapter explains how to configure the switch software features. There are four ways to access the switch: Serial console, Telnet/SSH, Web browser and SNMP.

Following topics are covered in this chapter:

4.1 Command Line Interface Introduction

The Command Line Interface (CLI) is one of the user interfaces to the switch's embedded software system. You can view the system information, show the status, configure the switch and receive a response back from the system by typing in a command.

There are different command modes each mode has its own access ability, available command lines and uses different command lines to enter and exit. These modes are User EXEC, Privileged EXEC, Global Configuration and (Port/VLAN) Interface Configuration modes.

User EXEC mode: As long as you log into the switch by CLI, you are in the User EXEC mode. You can ping, telnet remote device, and show some basic information.

Type **enable** to enter the next mode, **exit** to logout and **?** to see the command list

```
Switch>
  enable      Turn on privileged mode command
  exit        Exit current mode and down to previous mode
  list        Print command list
  ping        Send echo messages
  quit        Exit current mode and down to previous mode
  show        Show running system information
  telnet      Open a telnet connection
  traceroute  Trace route to destination
```

Privileged EXEC mode: Type **enable** in the User EXEC mode, then you can enter the Privileged EXEC mode. In this mode, the system allows you to view current configuration, reset default, reload switch, show system information, save configuration and enter the global configuration mode.

Type **configure terminal** to enter next mode, **exit** to leave and **?** to see the command list

```
Switch#
  archive     manage archive files
  clear       Reset functions
  clock       Configure time-of-day clock
  configure   Configuration from vty interface
  copy        Copy from one file to another
  debug       Debugging functions (see also 'undebug')
  disable     Turn off privileged mode command
  end         End current mode and change to enable mode
  exit        Exit current mode and down to previous mode
  list        Print command list
  more        Display the contents of a file
  no          Negate a command or set its defaults
  ping        Send echo messages
  quit        Exit current mode and down to previous mode
  reboot      Reboot system
  reload      copy a default-config file to replace the current one
  show        Show running system information
```

Global Configuration Mode: Type **configure terminal** in privileged EXEC mode and you will then enter global configuration mode. In global configuration mode, you can configure all the features that the system provides you.

Type **interface IFNAME/VLAN** to enter interface configuration mode, **exit** to leave and **?** to see the command list.

Available command lists of global configuration mode.

```
Switch# configure terminal
Switch(config)#
  access-list           Add an access list entry
  administrator         Administrator account setting
  arp                   Set a static ARP entry
  clock                 Configure time-of-day clock
  default               Set a command to its defaults
  end                   End current mode and change to enable mode
  exit                  Exit current mode and down to previous mode
  gvrp                  GARP VLAN Registration Protocol
  hostname              Set system's network name
  interface             Select an interface to configure
  ip                         IP information
  lacp                  Link Aggregation Control Protocol
  list                  Print command list
  log                   Logging control
  mac                   Global MAC configuration subcommands
  mac-address-table     mac address table
  mirror                Port mirroring
  no                         Negate a command or set its defaults
  ntp                   Configure NTP
  password              Assign the terminal connection password
  qos                   Quality of Service (QoS)
  relay                 relay output type information
  smtp-server           SMTP server configuration
  snmp-server           SNMP server
  spanning-tree         spanning tree algorithm
  super-ring            super-ring protocol
  trunk                 Trunk group configuration
  vlan                  Virtual LAN
  warning-event         Warning event selection
  write-config          Specify config files to write to
```

(Port) Interface Configuration: Type **interface IFNAME** in global configuration mode and you will then enter interface configuration mode, where you can configure port settings.

The port interface name for Fast Ethernet port 1 is fa1,… Fast Ethernet 7 is fa7, gigabit Ethernet port 8 is gi8.. Gigabit Ethernet port 10 is gi10. Type interface name accordingly when you want to enter certain interface configuration mode.

Type **exit** to leave.

Type **?** to see the command list

Available command lists of the global configuration mode.

```
Switch(config)# interface fa1
Switch(config-if)#
  acceptable           Configure 802.1Q acceptable frame types of a port.
  auto-negotiation     Enable auto-negotiation state of a given port
  description          Interface specific description
  duplex               Specify duplex mode of operation for a port
  end                  End current mode and change to enable mode
  exit                 Exit current mode and down to previous mode
  flowcontrol          Set flow-control value for an interface
  garp                 General Attribute Registration Protocol
  ingress                   802.1Q ingress filtering features
  lacp                 Link Aggregation Control Protocol
  list                 Print command list
  loopback             Specify loopback mode of operation for a port
  mac                  MAC interface commands
  mdix                 Enable mdix state of a given port
  no                   Negate a command or set its defaults
  qos                  Quality of Service (QoS)
  quit                 Exit current mode and down to previous mode
  rate-limit           Rate limit configuration
  shutdown             Shutdown the selected interface
  spanning-tree        spanning-tree protocol
  speed                Specify the speed of a Fast Ethernet port or a
Gigabit Ethernet port.
  switchport           Set switching mode characteristics
```

(VLAN) Interface Configuration: Press **interface VLAN VLAN-ID** in global configuration mode and you will then enter VLAN interface configuration mode, where you can configure the settings for the specific VLAN.

The VLAN interface name of VLAN 1 is VLAN 1, VLAN 2 is VLAN 2…

Type **exit** to leave the mode.   Type **?** to see the available command list.

The command lists of the VLAN interface configuration mode.

```
Switch(config)# interface vlan 1
Switch(config-if)#
  description     Interface specific description
  end             End current mode and change to enable mode
  exit            Exit current mode and down to previous mode
  ip              Interface Internet Protocol config commands
  list            Print command list
  no              Negate a command or set its defaults
  quit            Exit current mode and down to previous mode
  shutdown        Shutdown the selected interface
```

Summary of the 5 command modes.

Command Mode	**Main Function**	**Enter and Exit Method**	**Prompt**
User EXEC	This is the first level of access. User can ping, telnet remote device, and show some basic information	Enter: **Login** successfully Exit: **exit** to logout. Next mode: Type **enable** to enter privileged EXEC mode.	Switch>
Privileged EXEC	In this mode, the system allows you to view current configuration, reset default, reload switch, show system information, save configuration…and enter global configuration mode.	Enter: Type **enable** in User EXEC mode. Exec: Type **disable** to exit to user EXEC mode. Type **exit** to logout Next Mode: Type **configure terminal** to enter global configuration command.	Switch#
Global configuration	In global configuration mode, you can configure all the features that the system provides you	Enter: Type **configure terminal** in privileged EXEC mode Exit: Type **exit** or **end** or press **Ctrl-Z** to exit. Next mode: Type **interface IFNAME/ VLAN VID** to enter interface configuration mode	Switch(config)#
Port Interface configuration	In this mode, you can configure port related settings.	Enter: Type **interface IFNAME** in global configuration mode. Exit: Type **exit** or **Ctrl+Z** to global configuration mode. Type **end** to privileged EXEC mode.	Switch(config-if)#
VLAN Interface Configuration	In this mode, you can configure settings for specific VLAN.	Enter: Type **interface VLAN VID** in global configuration mode. Exit: Type **exit** or **Ctrl+Z** to global configuration mode. Type **end** to privileged EXEC mode.	Switch(config-vlan)#

Here are some useful commands to see available commands. It can save your time when typing and avoid errors.

? To see all the available commands in this mode. It helps you to see the next command you can/should type as well.

```
Switch(config)# interface (?)
  IFNAME  Interface's name
  vlan     Select a vlan to configure
```

(Character)? To see all the available commands starts from this character.

```
Switch(config)# a?
  access-list      Add an access list entry
  administrator    Administrator account setting
  arp         Set a static ARP entry
```

Tab This tab key helps you to input the command quicker. If there is only one available command in the next, clicking on tab key can help to finish typing soon.

```
Switch# co (tab) (tab)
Switch# configure terminal

Switch(config)# ac (tab)
Switch(config)# access-list
```

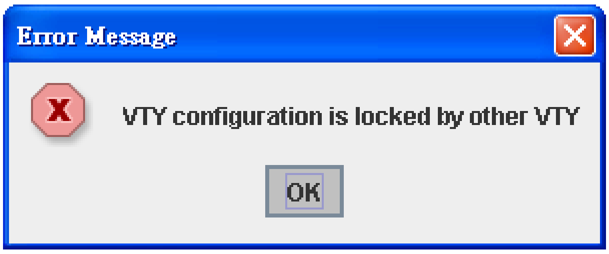
Ctrl+C To stop executing the unfinished command.

Ctrl+S To lock the screen of the terminal. You can't input any command.

Ctrl+Q To unlock the screen which is locked by Ctrl+S.

Ctrl+Z To exit configuration mode.

Alert message when multiple users want to configure the switch. If the administrator is in configuration mode, then the Web users can't change the settings. The switch allows only one administrator to configure the switch at a time.



VTY configuration is locked by other VTY

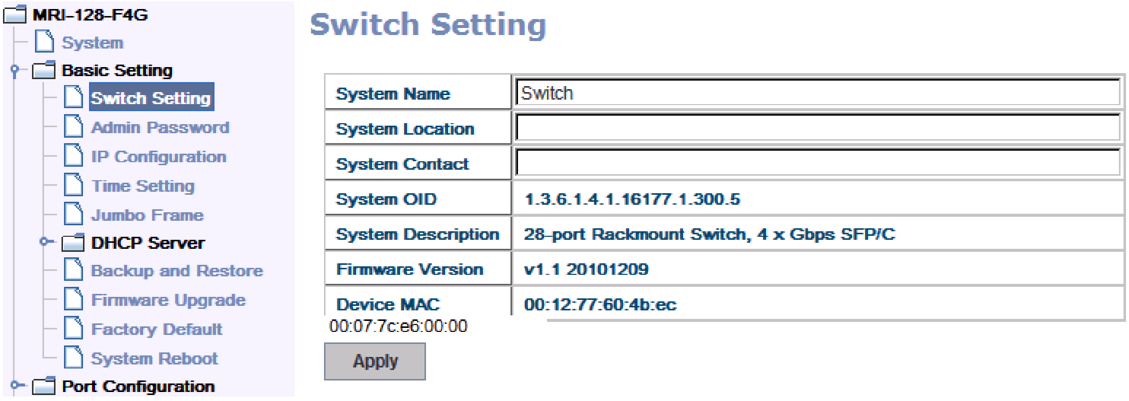
4.2 Basic Setting

The Basic Setting group provides you to configure switch information, IP address and User name/Password of the system. It also allows you to do firmware upgrade, backup and restore configuration, reload factory default and reboot the system.

Following commands are included in this chapter:

4.2.1 Switch Setting

You can assign System name, Location, Contact and view system information.



Switch Setting

System Name	Switch
System Location	
System Contact	
System OID	1.3.6.1.4.1.16177.1.300.5
System Description	28-port Rackmount Switch, 4 x Gbps SFP/C
Firmware Version	v1.1 20101209
Device MAC	00:12:77:60:4b:ec

00:07:7c:e6:00:00

System Name: You can assign a name to the switch. The available characters you can input is 64. After you configure the name, CLI system will select the first 12 characters as the name in CLI system.

System Location: You can specify the switch’s physical location here. The available characters you can input are 64.

System Contact: You can specify contact people here. You can type the name, mail address or other information of the administrator. The available characters you can input are 64.

System OID: The SNMP object ID of the switch. You can follow the path to find its private MIB in MIB browser. (**Note:** When you attempt to view private MIB, you should compile private MIB files into your MIB browser first.)

System Description: The name of this product.

Firmware Version: Display the firmware version installed in this device.

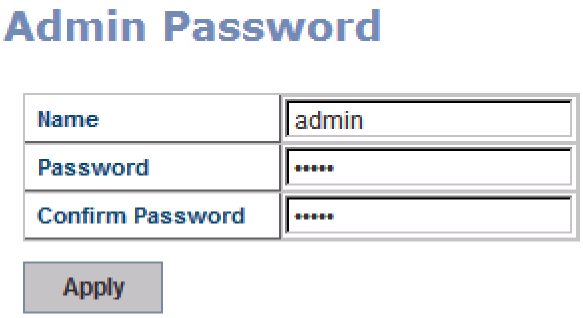
MAC Address: Display unique hardware address (MAC address) assigned by the manufacturer.

Once you finish the configuration, click on **Apply** to apply your settings.

Note: Always remember to select **Save** to save your settings. Otherwise, the settings you made will be lost when the switch is powered off.

4.2.2 Admin Password

You can change the user name and the password here to enhance security.



Admin Password

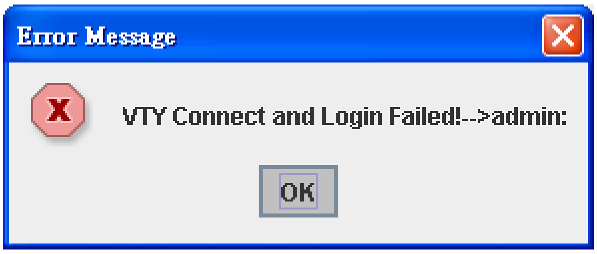
Name	admin
Password	•••••
Confirm Password	•••••

User name: You can type in a new user name here. The default setting is **admin**.

Password: You can type in a new password here. The default setting is **westermo**.

Confirm Password: You need to type the new password again to confirm it.

Once you finish configuring the settings, click on **Apply** to apply your configuration.

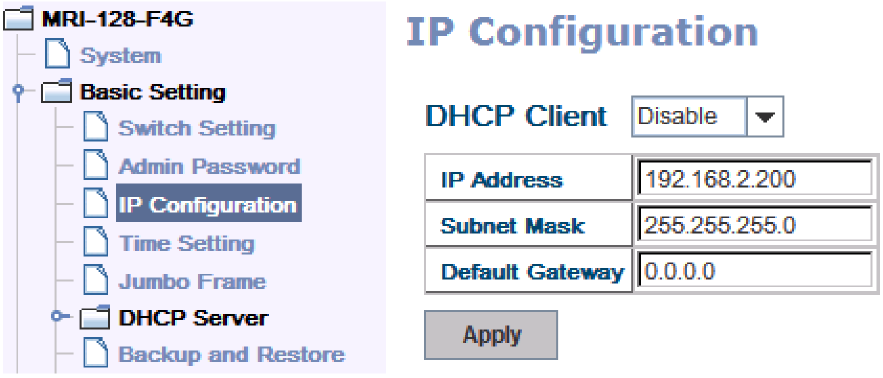


Error Message

VTY Connect and Login Failed!-->admin:

4.2.3 IP Configuration

This function allows users to configure the switch's IP address settings.



DHCP Client: Disable

IP Address	192.168.2.200
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0

DHCP Client: You can select to **Enable** or **Disable** DHCP Client function. When DHCP Client function is enabled, an IP address will be assigned to the switch from the network's DHCP server. In this mode, the default IP address will therefore be replaced by the one assigned by DHCP server. If DHCP Client is disabled, then the IP address that you specified will be used instead.

IP Address: You can assign the IP address reserved by your network for your switch. If DHCP Client function is enabled, you don't need to assign an IP address to the switch, as it will be overwritten by DHCP server and shown here. The default IP is 192.168.2.200.

Subnet Mask: You can assign the subnet mask for the IP address here. If DHCP Client function is enabled, you don't need to assign the subnet mask. The default Subnet Mask is 255.255.255.0.

Note: In the CLI, we use the enabled bit of the subnet mask to represent the number displayed in web UI. For example, 8 stands for 255.0.0.0; 16 stands for 255.255.0.0; 24 stands for 255.255.255.0.

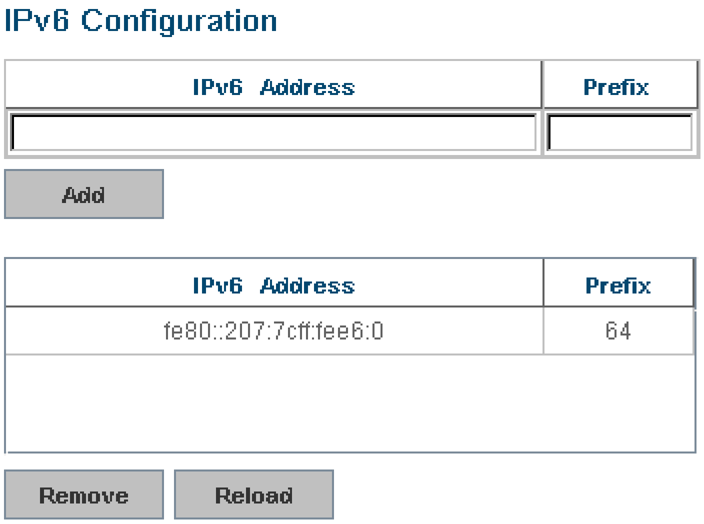
Default Gateway: You can assign the gateway for the switch here. **Note:** In CLI, we use 0.0.0.0/0 to represent for the default gateway.

Once you finish configuring the settings, click on **Apply** to apply your configuration.

IPv6 Configuration –An IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets). The groups are separated by colons (:), and the length of IPv6 address is 128bits.

An example of an IPv6 address is: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

The default IP address of MRI-128-F4G Managed Switch is assigned from MAC address, for example fe80:0:0:0:207:7cff:fee6:00, and the Leading zeroes in a group may be omitted. Thus, the example address may be written as: fe80::207:7cff:fe60:0.


IPv6 Configuration

IPv6 Address	Prefix

IPv6 Address	Prefix
fe80::207:7cff:fee6:0	64

IPv6 Address field: typing new IPv6 address in this field.

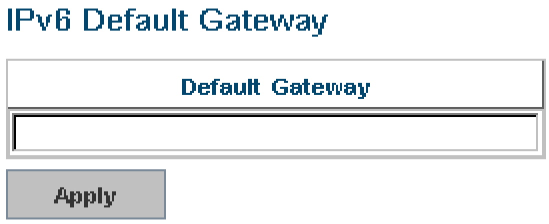
Prefix: the size of subnet or network, and it equivalent to the subnet mask, but written in different. The default subnet mask length is 64bits, and written in decimal value -64.

Add: after add new IPv6 address and prefix, don't forget click icon-"**Add**" to apply new address to system.

Remove: select existed IPv6 address and click icon-"**Remove**" to delete IP address.

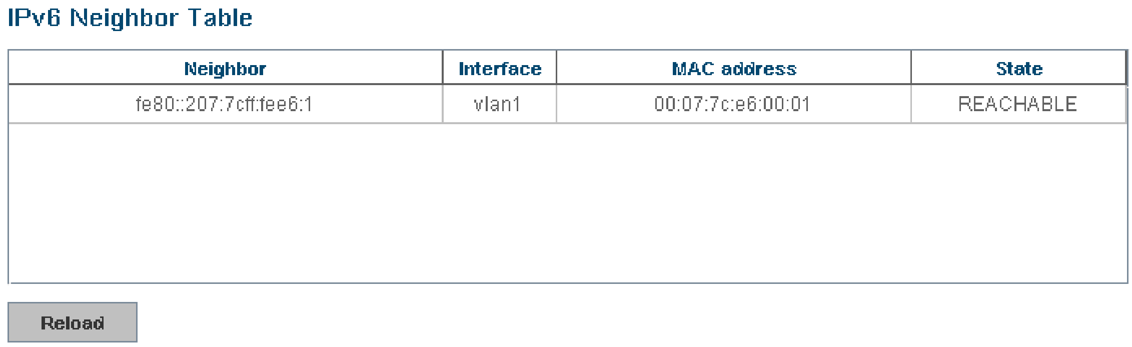
Reload: refresh and reload IPv6 address listing.

IPv6 Default Gateway: assign the IPv6 default gateway here. Type IPv6 address of the gateway then click "**Apply**". Note: In CLI, we user ::/0 to represent for the IPv6 default gateway.


IPv6 Default Gateway

Default Gateway

IPv6Neighbor Table: shows the IPv6 address of neighbor, connected interface, MAC address of remote IPv6 device, and current state of neighbor device.



IPv6 Neighbor Table

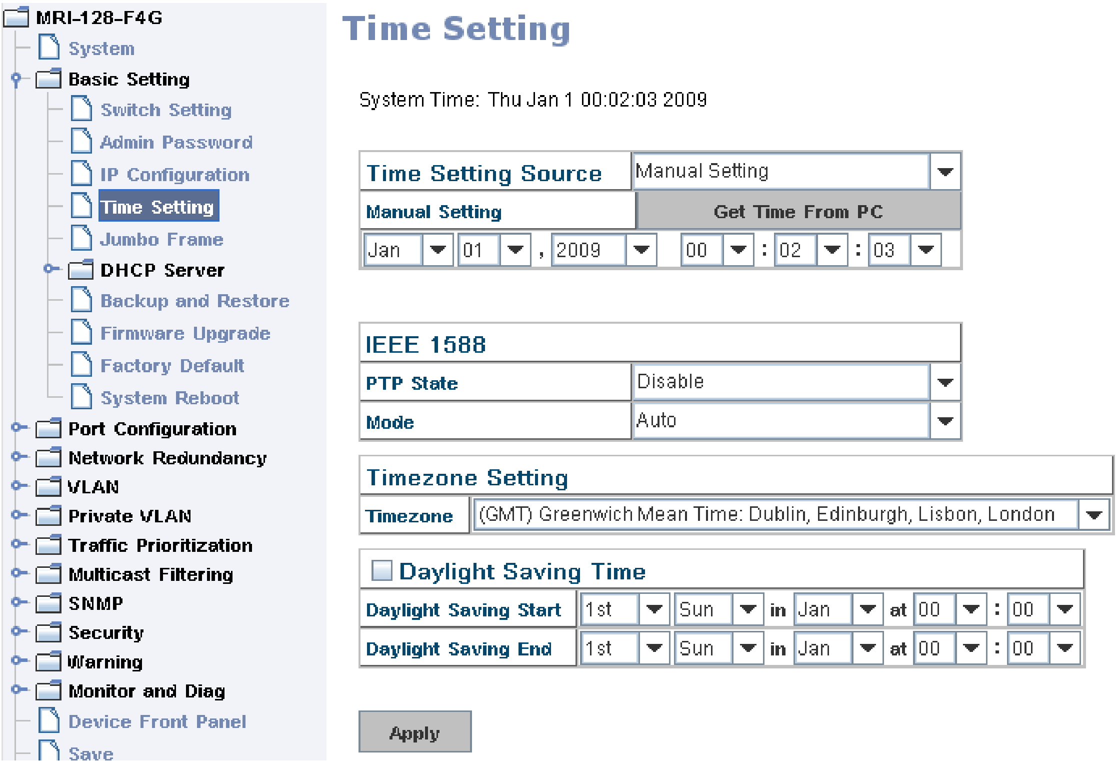
Neighbor	Interface	MAC address	State
fe80::207:7cff:fee6:1	vlan1	00:07:7c:e6:00:01	REACHABLE

The system will update IPv6 Neighbor Table automatically, and user also can click the icon "**Reload**" to refresh the table.

4.2.4 Time Setting

Time Setting source allow user to set the time manually or via a NTP server. Network Time Protocol (NTP) is used to synchronize computer clocks in a network. You can configure NTP settings here to synchronize the clocks of several switches on the network.

It also provides Daylight Saving Time function.



Time Setting

System Time: Thu Jan 1 00:02:03 2009

Time Setting Source	Manual Setting
Manual Setting	Get Time From PC
Jan 01 , 2009	00 : 02 : 03

IEEE 1588

PTP State	Disable
Mode	Auto

Timezone Setting

Timezone	(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

□ Daylight Saving Time

Daylight Saving Start	1st Sun in Jan at 00 : 00
Daylight Saving End	1st Sun in Jan at 00 : 00

Manual Setting: User can select "**Manual setting**" to change time as user wants. User also can click the button "**Get Time from PC**" to get PC's time setting for switch. After click the "**Get Time from PC**" and apply the setting, the System time display the same time as your PC's time.

NTP client: Set the Time Setting Source to NTP client to the NTP client service. NTP client will be automatically enabled if you change Time source to NTP Client. The system will send requests to acquire current time from the configured NTP server.

IEEE 1588: With the **Precision Time Protocol IEEE 1588** is a high-precision time protocol for synchronization used in control system on a network.

To enable IEEE 1588, select Enable in PTP Status and choose Auto, Master or Slave Mode. After time synchronized, the system time will display the correct time of the PTP server.

Time-zone: Select the time zone where the switch is located. Following table lists the time zones for different locations for your reference. The default time zone is GMT Greenwich Mean Time.

```
Switch(config)# clock timezone
   01   (GMT-12:00) Eniwetok, Kwajalein
   02   (GMT-11:00) Midway Island, Samoa
   03   (GMT-10:00) Hawaii
   04   (GMT-09:00) Alaska
   05   (GMT-08:00) Pacific Time (US & Canada) , Tijuana
   06   (GMT-07:00) Arizona
   07   (GMT-07:00) Mountain Time (US & Canada)
   08   (GMT-06:00) Central America
   09   (GMT-06:00) Central Time (US & Canada)
   10   (GMT-06:00) Mexico City
   11   (GMT-06:00) Saskatchewan
   12   (GMT-05:00) Bogota, Lima, Quito
   13   (GMT-05:00) Eastern Time (US & Canada)
   14   (GMT-05:00) Indiana (East)
   15   (GMT-04:00) Atlantic Time (Canada)
   16   (GMT-04:00) Caracas, La Paz
   17   (GMT-04:00) Santiago
   18   (GMT-03:00) NewFoundland
   19   (GMT-03:00) Brasilia
   20   (GMT-03:00) Buenos Aires, Georgetown
   21   (GMT-03:00) Greenland
   22   (GMT-02:00) Mid-Atlantic
   23   (GMT-01:00) Azores
   24   (GMT-01:00) Cape Verde Is.
```

25 (GMT) Casablanca, Monrovia

26 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

27 (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

28 (GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

29 (GMT+01:00) Brussels, Copenhagen, Madrid, Paris

30 (GMT+01:00) Sarajevo, Skopje, Sofija, Vilnius, Warsaw, Zagreb

31 (GMT+01:00) West Central Africa

32 (GMT+02:00) Athens, Istanbul, Minsk

33 (GMT+02:00) Bucharest

34 (GMT+02:00) Cairo

35 (GMT+02:00) Harare, Pretoria

36 (GMT+02:00) Helsinki, Riga, Tallinn

37 (GMT+02:00) Jerusalem

38 (GMT+03:00) Baghdad

39 (GMT+03:00) Kuwait, Riyadh

40 (GMT+03:00) Moscow, St. Petersburg, Volgograd

41 (GMT+03:00) Nairobi

42 (GMT+03:30) Tehran

43 (GMT+04:00) Abu Dhabi, Muscat

44 (GMT+04:00) Baku, Tbilisi, Yerevan

45 (GMT+04:30) Kabul

46 (GMT+05:00) Ekaterinburg

47 (GMT+05:00) Islamabad, Karachi, Tashkent

48 (GMT+05:30) Calcutta, Chennai, Mumbai, New Delhi

49 (GMT+05:45) Kathmandu

50 (GMT+06:00) Almaty, Novosibirsk

51 (GMT+06:00) Astana, Dhaka

52 (GMT+06:00) Sri Jayawardenepura

53 (GMT+06:30) Rangoon

54 (GMT+07:00) Bangkok, Hanoi, Jakarta

55 (GMT+07:00) Krasnoyarsk

56 (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi

57 (GMT+08:00) Irkutsk, Ulaan Bataar

58 (GMT+08:00) Kuala Lumpur, Singapore

59 (GMT+08:00) Perth

60 (GMT+08:00) Taipei

61 (GMT+09:00) Osaka, Sapporo, Tokyo

62 (GMT+09:00) Seoul

63	(GMT+09:00) Yakutsk
64	(GMT+09:30) Adelaide
65	(GMT+09:30) Darwin
66	(GMT+10:00) Brisbane
67	(GMT+10:00) Canberra, Melbourne, Sydney
68	(GMT+10:00) Guam, Port Moresby
69	(GMT+10:00) Hobart
70	(GMT+10:00) Vladivostok
71	(GMT+11:00) Magadan, Solomon Is., New Caledonia
72	(GMT+12:00) Aukland, Wellington
73	(GMT+12:00) Fiji, Kamchatka, Marshall Is.
74	(GMT+13:00) Nuku'alofa

Daylight Saving Time: Set when Enable Daylight Saving Time start and end, during the Daylight Saving Time, the device's time is one hour earlier than the actual time.

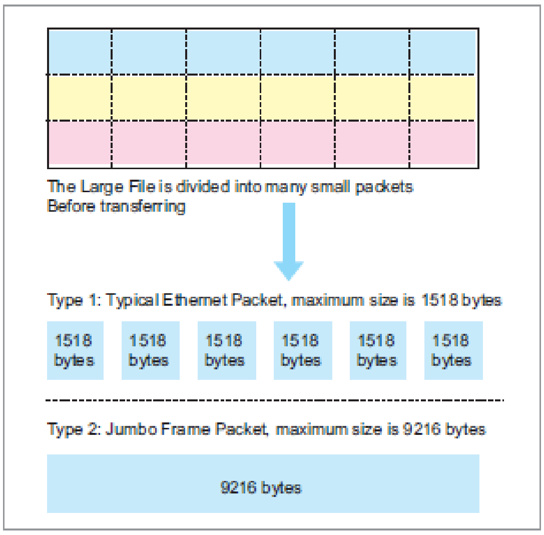
Daylight Saving Start and **Daylight Saving End**: the time setting allows user to selects the week that monthly basis, and sets the End and Start time individually.

Once you finish your configuration, click on **Apply** to apply your configuration.

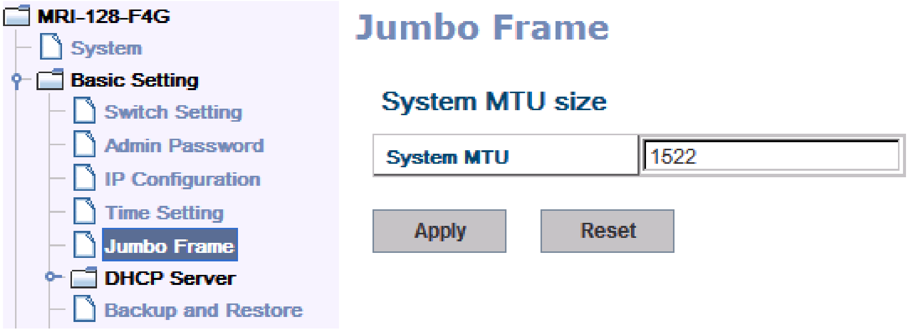
4.2.5 Jumbo Frame

What is Jumbo Frame?

The typical Ethernet frame is range from 64 to 1518 bytes. This is sufficient for general usages. However, when users want to transmit large files, the files may be divided into many small size packets. While the transmitting speed becomes slow, long size Jumbo frame can solve the issue.


The Large File is divided into many small packets
Before transferring
Type 1: Typical Ethernet Packet, maximum size is 1518 bytes
1518 bytes
1518 bytes
1518 bytes
1518 bytes
1518 bytes
1518 bytes
Type 2: Jumbo Frame Packet, maximum size is 9216 bytes
9216 bytes

The switch allows you configure the size of the MTU, Maximum Transmission Unit. The default value is 1,518bytes. The maximum Jumbo Frame size is 9,216 bytes.



Jumbo Frame

System MTU size

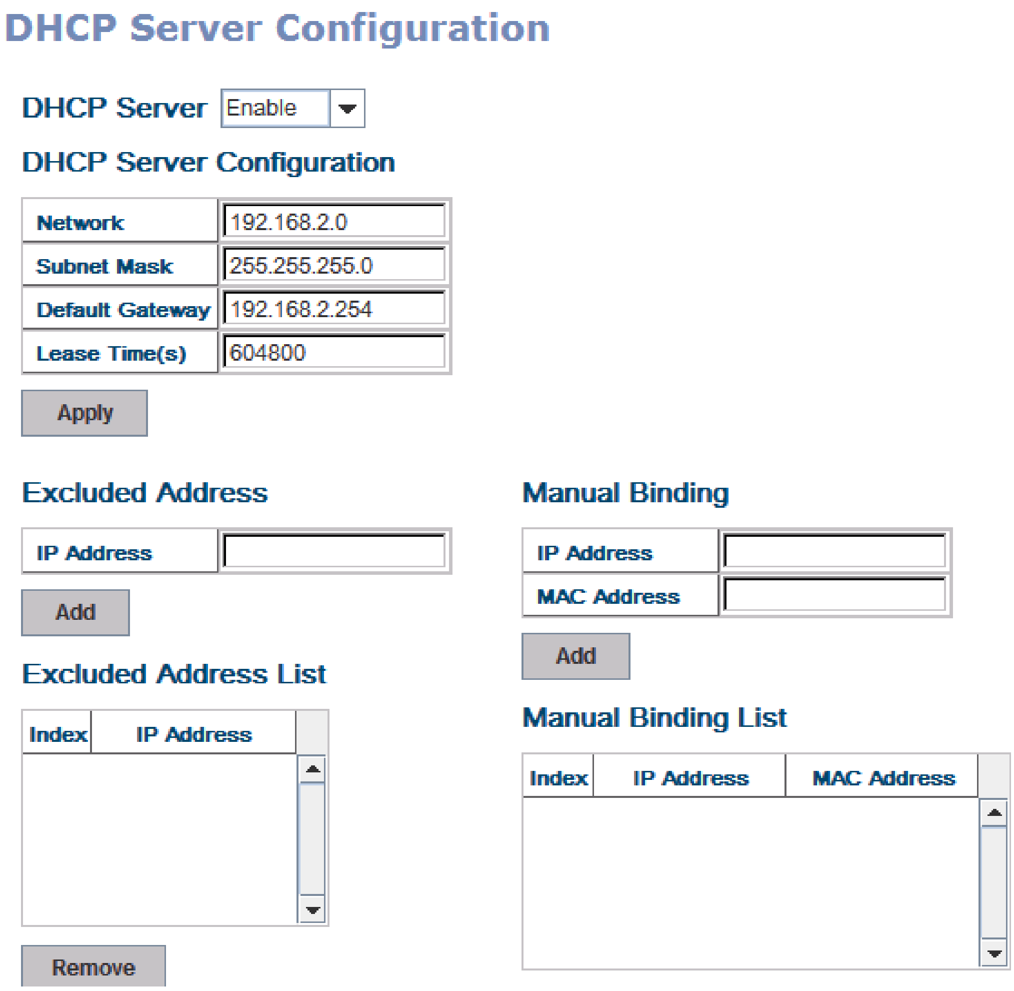
System MTU	1522

Once you finish your configuration, click on **Apply** to apply your configuration.

4.2.6 DHCP Server

You can select to **Enable** or **Disable** DHCP Server function. It will assign a new IP address to link partners.

DHCP Server configuration



DHCP Server Configuration

DHCP Server: Enable

DHCP Server Configuration

Network	192.168.2.0
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.254
Lease Time(s)	604800

Excluded Address

IP Address	

Excluded Address List

Index	IP Address

Manual Binding

IP Address	
MAC Address	

Manual Binding List

Index	IP Address	MAC Address

After selecting to enable DHCP Server function, type in the Network IP address for the DHCP server IP pool, Subnet Mask, Default Gateway address and Lease Time for client.

Once you have finished the configuration, click **Apply** to apply your configuration

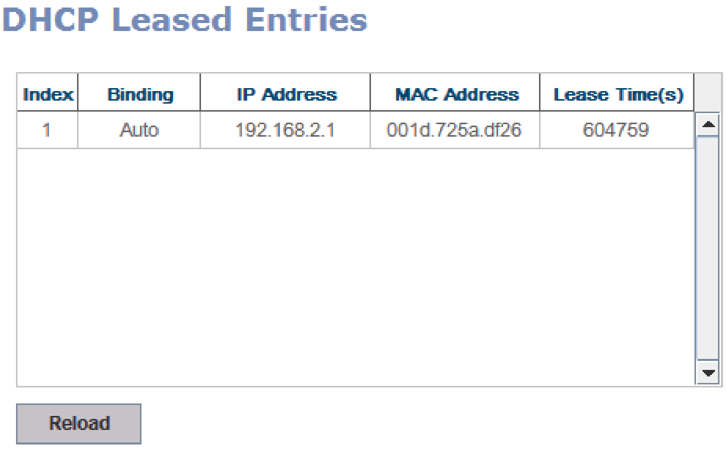
Excluded Address:

You can type a specific address into the **IP Address field** for the DHCP server reserved IP address.

The IP address that is listed in the **Excluded Address List Table** will not be assigned to the network device. Add or remove an IP address from the **Excluded Address List** by clicking **Add** or **Remove**.

Manual Binding: the switch provides a MAC address and IP address binding and removing function. You can type in the specified IP and MAC address, then click **Add** to add a new MAC&IP address binding rule for a specified link partner, like PLC or any device without **DHCP client** function. To remove from the binding list, just select the rule to remove and click **Remove**.

DHCP Leased Entries: *the switch* provides an assigned IP address list for user check. It will show the MAC and IP address that was assigned by *the switch*. Click the **Reload** button to refresh the listing.



DHCP Leased Entries

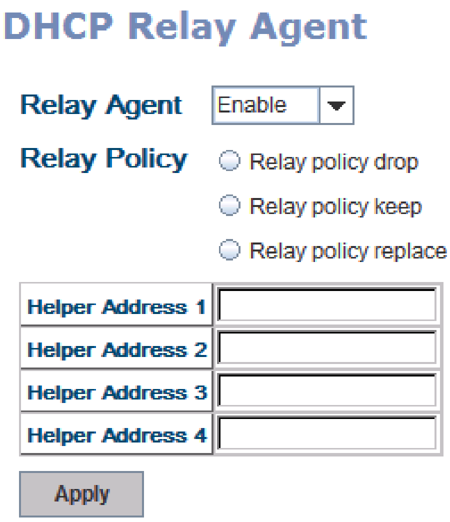
Index	Binding	IP Address	MAC Address	Lease Time(s)
1	Auto	192.168.2.1	001d.725a.df26	604759

DHCP Relay Agent: The DHCP Relay Agent is also known as DHCP Option 82. It can help relay the DHCP Request to remote DHCP server located in different subnet.

Note: The DHCP Server cannot work with DHCP Relay Agent at the same time.

Relay Agent: Choose Enable or Disable the relay agent.

Relay Policy: The Relay Policy is used when the DHCP request is relayed through more than one switch. The switch can drop, keep or replace the MAC address of the DHCP Request packet.



DHCP Relay Agent

Relay Agent: Enable

Relay Policy:
○ Relay policy drop
○ Relay policy keep
○ Relay policy replace

Helper Address 1	
Helper Address 2	
Helper Address 3	
Helper Address 4	

Helper Address: Type the IP address of the target DHCP Server. There are 4 available IP addresses.

4.2.7 Backup and Restore

With Backup command, you can save current configuration file saved in the switch's flash to admin PC or TFTP server. This will allow you to go to **Restore** command later to restore the configuration file back to the switch. Before you restore the configuration file, you must place the backup configuration file in the PC or TFTP server. The switch will then download this file back to the flash.

There are 2 modes for users to backup/restore the configuration file, Local File mode and TFTP Server mode.

Local File mode: In this mode, the switch acts as the file server. Users can browse the target folder and then type the file name to backup the configuration. Users can also browse the target folder and select existed configuration file to restore the configuration back to the switch. This mode is only provided by Web UI while CLI is not supported.

TFTP Server mode: In this mode, the switch acts as TFTP client. Before you do so, make sure that your TFTP server is ready. Then please type the IP address of TFTP Server and Backup configuration file name. This mode can be used in both CLI and Web UI.

TFTP Server IP Address: You need to key in the IP address of your TFTP Server here.

Backup/Restore File Name: Please type the correct file name of the configuration file..

Configuration File: The configuration file of the switch is a pure text file. You can open it by word/txt read file. You can also modify the file, add/remove the configuration settings, and then restore back to the switch.

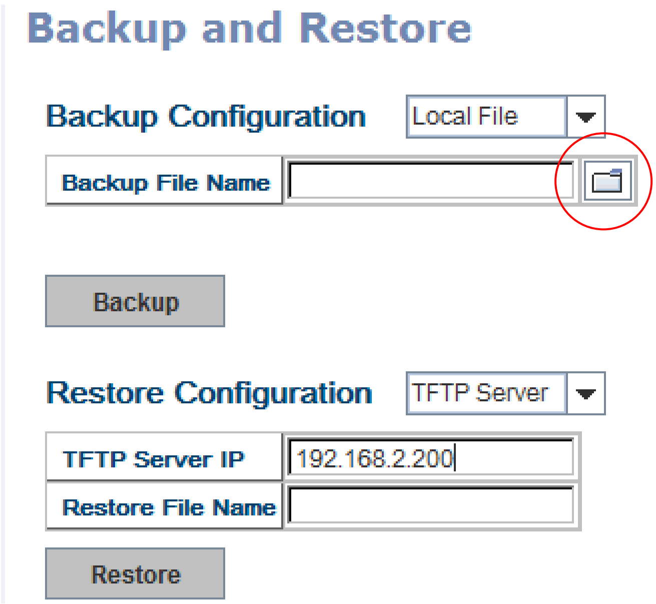
Startup Configuration File: After you saved the running-config to flash, the new settings will be kept and work after power cycle. You can use *show startup-config* to view it in CLI. The Backup command can only backup such configuration file to your PC or TFTP server.

Technical Tip:

Default Configuration File: *The switch provides the default configuration file in the system. You can use Reset button, Reload command to reset the system.*

Running Configuration File: *The switch's CLI allows you to view the latest settings running by the system. The information shown here is the settings you set up but haven't saved to flash. The settings not yet saved to flash will not work after power recycle. You can* use *show running-config* to view it in CLI.

Once you finish selecting and configuring the settings, click on **Backup** or **Restore** to run



Backup and Restore

Backup Configuration: Local File

Backup File Name:

Restore Configuration: TFTP Server

TFTP Server IP: 192.168.2.200

Restore File Name:

Click on Folder icon to select the target file you want to backup/restore.

Note that the folders of the path to the target file do not allow you to input space key.

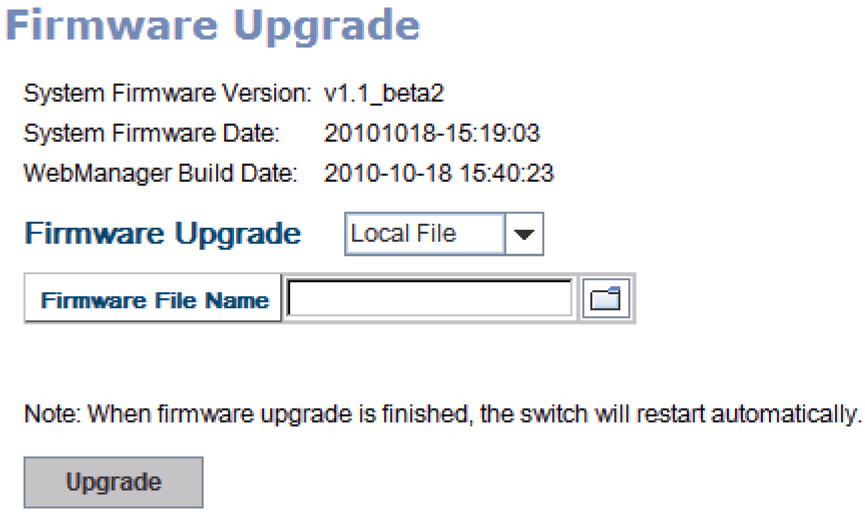
Type the IP address of TFTP Server IP. Then click on **Backup/Restore**.

Note: point to the wrong file will cause the entire configuration missed

4.2.8 Firmware Upgrade

In this section, you can update the latest firmware for your switch. Westermo provides the latest firmware in the Web site. The new firmware may include new features, bug fixes or other software changes. We'll also provide the release notes for the update as well. For technical viewpoint, we suggest you use the latest firmware before installing the switch to the customer site.

Note that the system will be automatically rebooted after you finished upgrading new firmware. Please remind the attached users before you do this.



Firmware Upgrade

System Firmware Version: v1.1_beta2

System Firmware Date: 20101018-15:19:03

WebManager Build Date: 2010-10-18 15:40:23

Firmware Upgrade: Local File

Firmware File Name:

Note: When firmware upgrade is finished, the switch will restart automatically.

There are two modes for users to backup/restore the configuration file, Local File mode and TFTP Server mode.

Local File mode: In this mode, the switch acts as the file server. Users can browse the target folder and then type the file name to backup the configuration. Users also can browse the target folder and select the existed configuration file to restore the configuration back to the switch. This mode is only provided by Web UI while CLI is not supported.

TFTP Server mode: In this mode, the switch acts as the TFTP client. Before you do so, make sure that your TFTP server is ready. And then please type the IP address of TFTP Server IP address. This mode can be used in both CLI and Web UI.

TFTP Server IP Address: You need to key in the IP address of your TFTP Server here.

Firmware File Name: The file name of the new firmware.

The UI also shows you the current firmware version and built date of current firmware. Please check the version number after the switch is rebooted.

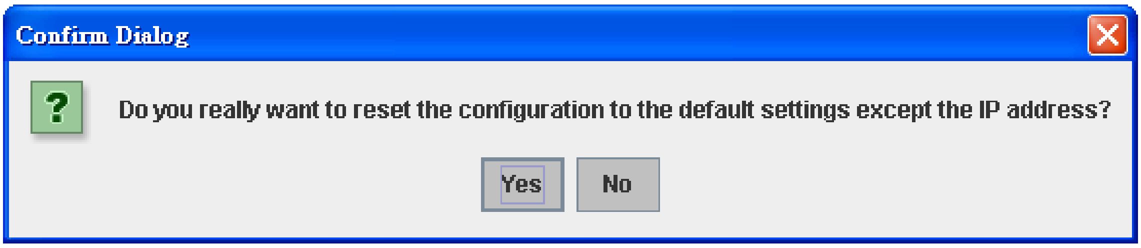
Before upgrading firmware, please check the file name and switch model name first and carefully. The switch provide protection when upgrading incorrect firmware file, the system would not crash even download the incorrect firmware. Even we have the protection, we still ask you don’t try/test upgrade incorrect firmware, the unexpected event may occur or damage the system.

After finishing transmitting the firmware, the system will copy the firmware file and replace the firmware in the flash. The CLI show …… until the process is finished.

4.2.9 Factory Default

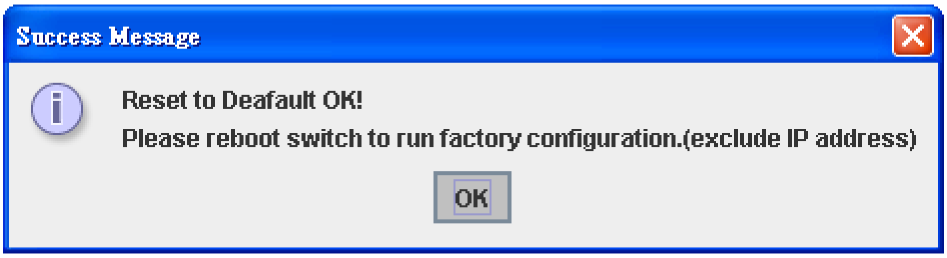
In this section, you can reset all the configurations of the switch to default setting. Click on **Reset** the system will then reset all configurations to default setting. The system will show you popup message window after finishing this command. Default setting will work after rebooting the switch.

Popup alert screen to confirm the command. Click on **Yes** to start it.



Do you really want to reset the configuration to the default settings except the IP address?

Click on **OK** to close the screen. Then please go to **Reboot** page to reboot the switch.



Reset to Deafault OK!
Please reboot switch to run factory configuration.(exclude IP address)

Click on **OK.** The system will then auto reboot the device.

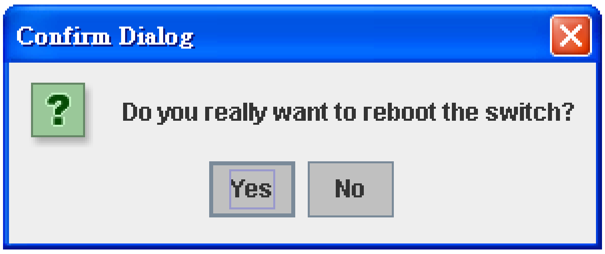
Note: If you already configured the IP of your device to other IP address, when you use this command by CLI and Web User Interface, the switch will not reset the IP address to default IP. The system will remain the IP address so that you can still connect the switch via the network.

4.2.10 System Reboot

System Reboot allows you to reboot the device. Some of the feature changes require you to reboot the system. Click on **Reboot** to reboot your device.

Note: Remember to click on **Save** button to save your settings. Otherwise, the settings you made will be gone when the switch is powered off.

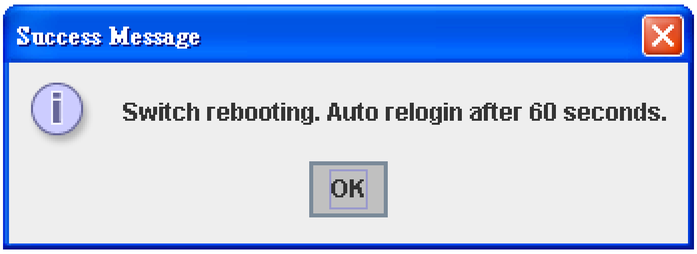
Pop-up alert screen to request confirmation. Click on **Yes**. Then the switch will be rebooted immediately.



Confirm Dialog

Do you really want to reboot the switch?

Pop-up message screen appears when rebooting the switch..



Success Message

Switch rebooting. Auto relogin after 60 seconds.

Note: Since different browser may has different behavior. If the Web GUI doesn’t re-login, please manually type the IP Address and log into the switch again.

4.2.11 CLI Commands for Basic Setting

Feature	Command Line
Switch Setting	
System Name	Switch(config)# hostname WORD Network name of this system Switch(config)# hostname SWITCH SWITCH(config)#
System Location	SWITCH(config)# snmp-server location Sweden
System Contact	SWITCH(config)# snmp-server contact support@westermo.se
Display	SWITCH# show snmp-server name SWITCH SWITCH# show snmp-server location Sweden SWITCH# show snmp-server contact support@westermo.se Switch> show version Loader Version : 1.0.0.3

	Firmware Version : 1.1.26-20101025-10:17:48 Switch# show hardware mac MAC Address : 00:07:7c:e6:00:00 Switch# show hardware led RM : Off
Admin Password	
User Name and Password	SWITCH(config)# administrator NAME Administrator account name SWITCH(config)# administrator super PASSWORD Administrator account password SWITCH(config)# administrator super super Change administrator account super and password super success.
Display	SWITCH# show administrator Administrator account information name: super password: super
IP Configuration	
IP Address/Mask (192.168.2.8, 255.255.255.0	SWITCH(config)# int vlan 1 SWITCH(config-if)# ip address dhcp SWITCH(config-if)# ip address 192.168.2.8/24 **(DHCP Client)** SWITCH(config-if)# ip dhcp client SWITCH(config-if)# ip dhcp client renew
Gateway	SWITCH(config)# ip route 0.0.0.0/0 192.168.2.254/24
Remove Gateway	SWITCH(config)# no ip route 0.0.0.0/0 192.168.2.254/24

Display	SWITCH# show interface vlan1
	interface vlan1 is up, line protocol detection is disabled
	    index 22 metric 1 mtu 1500 <…>
	    HWaddr: 00:07:7c:ff:13:57
	    inet 192.168.2.8/24 broadcast 192.168.2.255
	    ……….
	
	SWITCH# show running-config

	……… ! interface vlan1 ip address 192.168.2.8/24 no shutdown ! ip route 0.0.0.0/0 192.168.2.254/24 !
Time Setting	

NTP Server	SWITCH(config)# ntp peer
	    enable
	    disable
	    primary
	    secondary
	SWITCH(config)# ntp peer primary
	    IPADDR
	SWITCH(config)# ntp peer primary 192.168.2.200

Time Zone	SWITCH(config)# clock timezone 26 Sun Jan 1 04:13:24 2006 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London **Note:** By typing clock timezone ?, you can see the timezone list. Then choose the number of the timezone you want to select.

IEEE 1588	Switch(config)# ptpd run
	    <cr>
	    preferred-clock Preferred Clock
	    slave Run as slave

Display	SWITCH# sh ntp associations Network time protocol Status : Disabled Primary peer : N/A Secondary peer : N/A SWITCH# show clock Sun Jan 1 04:14:19 2006 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

	SWITCH# show clock timezone clock timezone (26) (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London Switch# show ptpd PTPd is enabled Mode: Slave
Jumbo Frame	
Jumbo Frame	Type the maximum MTU to enable Jumbo Frame: SWITCH(config)# system mtu <64-9216> bytes (with VLAN tag) Switch(config)# system mtu 9216 Disable Jumbo Frame: SWITCH(config)# no system mtu
Display	SWITCH# show system mtu System MTU size is 9216 bytes After disabled Jumbo Frame: SWITCH# show system mtu System MTU size is 1522 bytes
DHCP	

DHCP Commands	Switch(config)# router dhcp
	Switch(config-dhcp)#
	    default-router DHCP Default Router
	    end Exit current mode and down to previous enable mode
	    exit Exit current mode and down to previous mode
	    ip IP protocol
	    lease DHCP Lease Time
	    list Print command list
	    network dhcp network
	    no remove
	    quit Exit current mode and down to previous mode
	    service enable service

DHCP Server Enable	Switch(config-dhcp)# service dhcp

	<cr>
DHCP Server IP Pool (Network/Mask)	Switch(config-dhcp)# network A.B.C.D/M network/mask ex. 10.10.1.0/24 Switch(config-dhcp)# network 192.168.2.0/24
DHCP Server – Default Gateway	Switch(config-dhcp)# default-router A.B.C.D address Switch(config-dhcp)# default-router 192.168.2.254
DHCP Server – lease time	Switch(config-dhcp)# lease TIME second Switch(config-dhcp)# lease 1000 (1000 second)
DHCP Server – Excluded Address	Switch(config-dhcp)# ip dhcp excluded-address A.B.C.D IP address Switch(config-dhcp)# ip dhcp excluded-address 192.168.2.20023 <cr>
DHCP Server – Static IP and MAC binding	Switch(config-dhcp)# ip dhcp static MACADDR MAC address Switch(config-dhcp)# ip dhcp static 0007.7c00.0001 A.B.C.D leased IP address Switch(config-dhcp)# ip dhcp static 0007.7c00.0001192.168.2.99
DHCP Relay – Enable DHCP Relay	Switch(config-dhcp)# ip dhcp relay information option Option82 policy Option82 Switch(config-dhcp)# ip dhcp relay information option
DHCP Relay – DHCP policy	Switch(config-dhcp)# ip dhcp relay information policy drop Relay Policy keep Drop/Keep/Replace option82 field replace Switch(config-dhcp)# ip dhcp relay information policy drop <cr> Switch(config-dhcp)# ip dhcp relay information policy keep <cr> Switch(config-dhcp)# ip dhcp relay information policy replace <cr>
DHCP Relay – IP Helper Address	Switch(config-dhcp)# ip dhcp helper-address A.B.C.D Switch(config-dhcp)# ip dhcp helper-address 192.168.2.200
Reset DHCP Settings	Switch(config-dhcp)# ip dhcp reset <cr>

DHCP Server Information	Switch# show ip dhcp server statistics DHCP Server ON Address Pool 1 network:192.168.2.0/24 default-router:192.168.2.254 lease time:604800 Excluded Address List IP Address --------------- 192.168.2.200 Manual Binding List IP Address MAC Address --------------- -------------- 192.168.2.99 0007.7c01.0203 Leased Address List IP Address MAC Address Leased Time Remains --------------- -------------- --------------------
DHCP Relay Information	Switch# show ip dhcp relay DHCP Relay Agent ON -- IP helper-address : 192.168.2.200 Re-forwarding policy: Replace
Backup and Restore	
Backup Startup Configuration file	Switch# copy startup-config tftp: 192.168.2.33/default.conf Writing Configuration [OK] ***Note 1:*** *To backup the latest startup configuration file, you should save current settings to flash first. You can refer to 4.12 to see how to save settings to the flash.* *Note 2: 192.168.2.33 is the TFTP server's IP and default.conf is name of the configuration file. Your environment may use different IP addresses or different file name. Please type target TFTP server IP or*

	file name in this command.
Restore Configuration	Switch# copy tftp: 192.168.2.33/default.conf startup-config
Show Startup Configuration	Switch# show startup-config
Show Running Configuration	Switch# show running-config
Firmware Upgrade	
Firmware Upgrade	Switch# archive download-sw /overwrite tftp 192.168.2.33 MRI-128-F4G.bin Firmware upgrading, don't turn off the switch! Tftping file MRI-128-F4G.bin Firmware upgrading .... Firmware upgrade success!! Rebooting.......
Factory Default	
Factory Default	Switch# reload default-config file Reload OK! Switch# reboot
System Reboot	
Reboot	Switch# reboot

4.3 Port Configuration

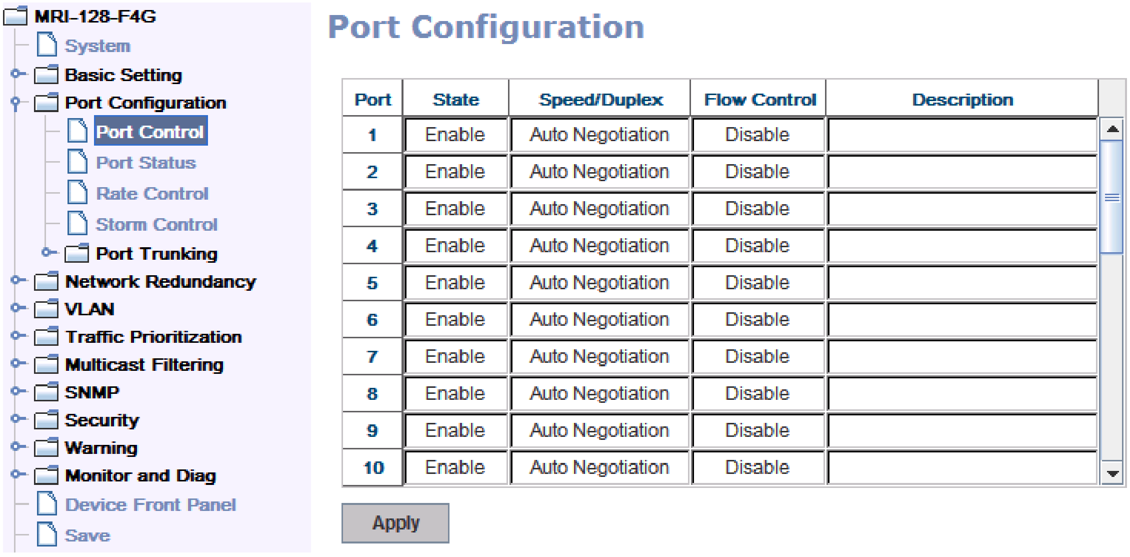
Port Configuration group enables you to enable/disable port state, or configure port auto-negotiation, speed, and duplex, flow control, rate limit control and port aggregation settings. It also allows you to view port status and aggregation information.

Following commands are included in this chapter:

4.3.1 Port Control
4.3.2 Port Status
4.3.3 Rate Control
4.3.4 Storm Control
4.3.5 Port Trunking
4.3.6 Command Lines for Port Configuration

4.3.1 Port Control

Port Control commands allow you to enable/disable port state, or configure the port auto-negotiation, speed, duplex and flow control.



Port Configuration

Port	State	Speed/Duplex	Flow Control	Description
1	Enable	Auto Negotiation	Disable	
2	Enable	Auto Negotiation	Disable	
3	Enable	Auto Negotiation	Disable	
4	Enable	Auto Negotiation	Disable	
5	Enable	Auto Negotiation	Disable	
6	Enable	Auto Negotiation	Disable	
7	Enable	Auto Negotiation	Disable	
8	Enable	Auto Negotiation	Disable	
9	Enable	Auto Negotiation	Disable	
10	Enable	Auto Negotiation	Disable	

Select the port you want to configure and make changes to the port.

In **State** column, you can enable or disable the state of this port. Once you disable the port stop to link to the other end and stop to forward any traffic. The default setting is Enable which means all the ports are workable when you receive the device.

In **Speed/Duplex** column, you can configure port speed and duplex mode of this port. Below are the selections you can choose:

Fast Ethernet Port 1~24 (fa1~fa24): Auto Negotiation, 10M Full Duplex(10 Full), 10M Half Duplex(10 Half), 100M Full Duplex(100 Full) and 100M Half Duplex(100 Half).

Gigabit Ethernet Combo Port 25~28: (gi25~gi28): Auto Negotiation, 10M Full Duplex(10 Full), 10M Half Duplex(10 Half), 100M Full Duplex(100 Full), 100M Half Duplex(100 Half), 1000M Full Duplex(1000 Full), 1000M Half Duplex(1000 Half).

The default mode is Auto Negotiation mode.

Note: The on board Gigabit SFP port (SFP 25, 26, 27 and 28) in the switch only support 1000M Full mode.

In **Flow Control** column, "Symmetric" means that you need to activate the flow control function of the remote network device in order to let the flow control of that corresponding port on the switch to work. "Disable" means that you don't need to activate the flow control function of the remote network device, as the flow control of that corresponding port on the switch will work anyway.

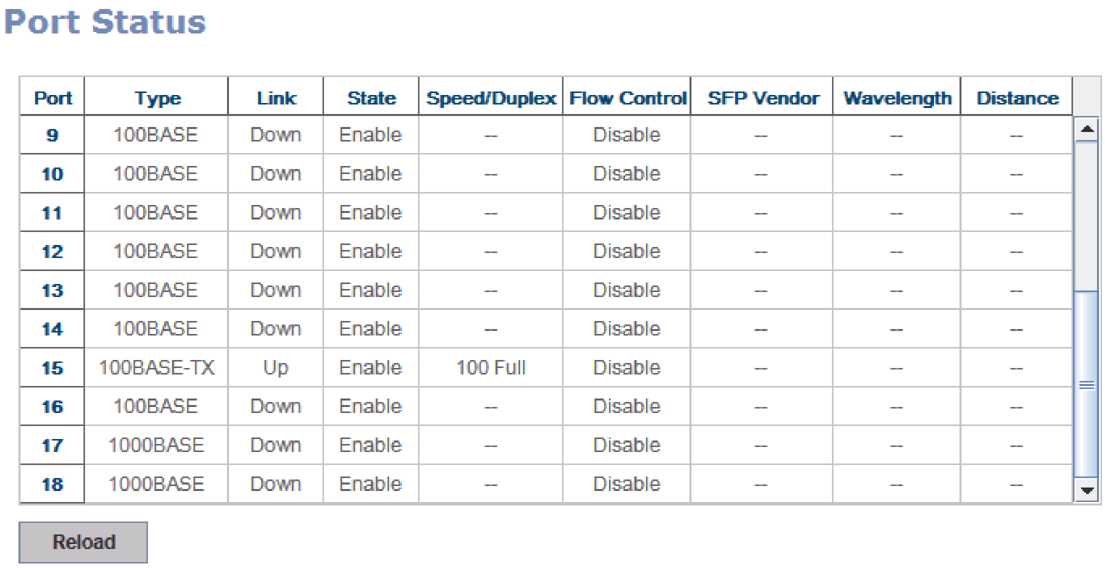
In **Description** column, you can add description for the port. You can know the target it attached to easier in remote.

Once you finish configuring the settings, click on **Apply** to save the configuration.

Technical Tips: *If both ends are not at the same speed, they can't link with each other. If both ends are not in the same duplex mode, they will be connected by half mode.*

4.3.2 Port Status

Port Status shows you current port status.



Port Status

Port	Type	Link	State	Speed/Duplex	Flow Control	SFP Vendor	Wavelength	Distance
9	100BASE	Down	Enable	--	Disable	--	--	--
10	100BASE	Down	Enable	--	Disable	--	--	--
11	100BASE	Down	Enable	--	Disable	--	--	--
12	100BASE	Down	Enable	--	Disable	--	--	--
13	100BASE	Down	Enable	--	Disable	--	--	--
14	100BASE	Down	Enable	--	Disable	--	--	--
15	100BASE-TX	Up	Enable	100 Full	Disable	--	--	--
16	100BASE	Down	Enable	--	Disable	--	--	--
17	1000BASE	Down	Enable	--	Disable	--	--	--
18	1000BASE	Down	Enable	--	Disable	--	--	--

The description of the columns is as below:

Port: Port interface number.

Type: 100BASE-TX -> Fast Ethernet copper port. 100BASE-FX -> 100Base-FX Fiber Port. 1000BASE-TX -> Gigabit Ethernet Copper port. 1000BASE-X-> Gigabit Fiber Port

Link: Link status. Up -> Link UP. Down -> Link Down.

State: Enable -> State is enabled. Disable -> The port is disable/shutdown.

Speed/Duplex: Current working status of the port.

Flow Control: The state of the flow control.

SFP Vendor: Vendor name of the SFP transceiver you plugged. Apply to fiber port.

Wavelength: The wave length of the SFP transceiver you plugged. Apply to fiber port.

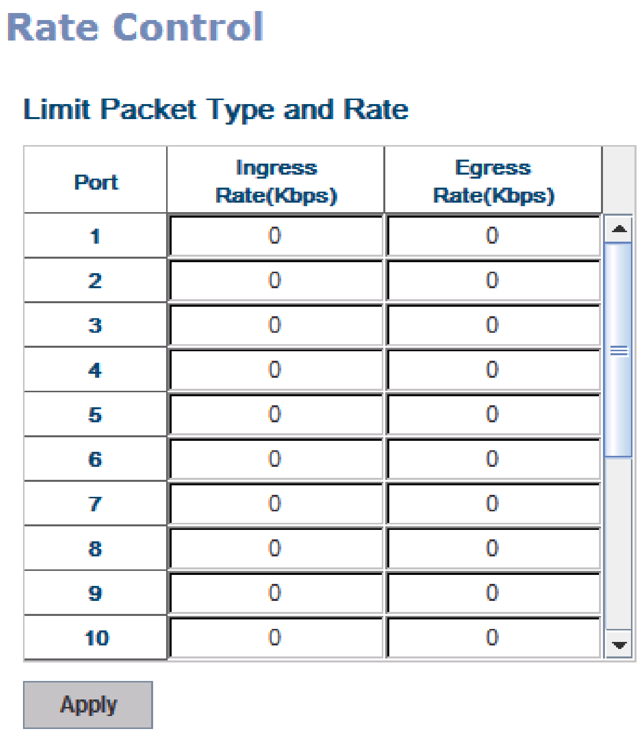
Distance: The transmission distance of the SFP transceiver you plugged. Apply to fiber port.

Note: Most of the SFP transceivers provide vendor information which allows your switch to read it. The User Interface can display vendor name, wave length and distance of all Westermo SFP transceiver family. If you see Unknown info, it may mean that the vendor doesn't provide their information or that the information of their transceiver can't be read.

4.3.3 Rate Control

Rate limiting is a form of flow control used to enforce a strict bandwidth limit at a port. You can program separate transmit (Egress Rule) and receive (Ingress Rule) rate limits at each port, and even apply the limit to certain packet types as described below.

The figure shows you the Limit Rate of Ingress and Egress. You can type the volume in the blank. The volume of the switch is step by 8Kbps.



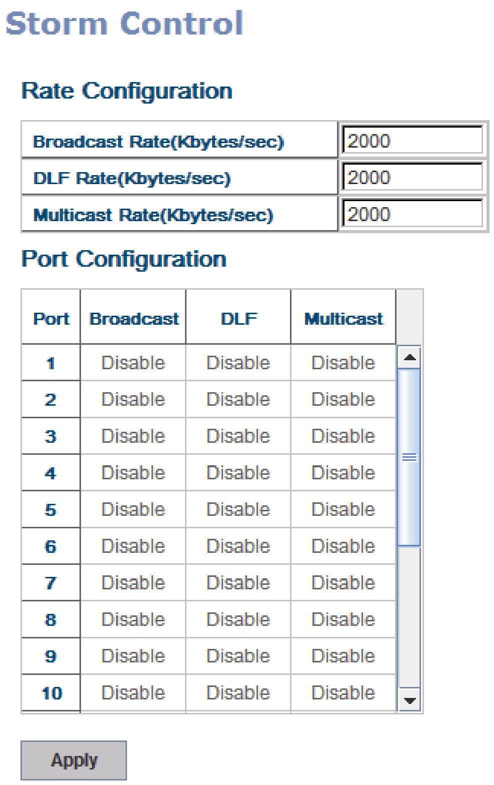
Rate Control

Limit Packet Type and Rate

Port	Ingress Rate(Kbps)	Egress Rate(Kbps)
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0

4.3.4 Storm Control

The Storm Control is similar to Rate Control. Rate Control filters all the traffic over the threshold you input by User Interface. Storm Control allows user to define the rate for specific Packet Types.



Storm Control

Rate Configuration

Broadcast Rate(Kbytes/sec)	2000
DLF Rate(Kbytes/sec)	2000
Multicast Rate(Kbytes/sec)	2000

Port Configuration

Port	Broadcast	DLF	Multicast
1	Disable	Disable	Disable
2	Disable	Disable	Disable
3	Disable	Disable	Disable
4	Disable	Disable	Disable
5	Disable	Disable	Disable
6	Disable	Disable	Disable
7	Disable	Disable	Disable
8	Disable	Disable	Disable
9	Disable	Disable	Disable
10	Disable	Disable	Disable

Packet type: You can assign the Rate for specific packet types based on packet number per second. The packet types of the Ingress Rule listed here include **Broadcast, DLF (Destination Lookup Failure) and Multicast**. Choose **Enable/Disable** to enable or disable the storm control of specific port.

Rate: This column allows you to manually assign the limit rate of the port. The unit is packets per second. The limit range is from 1 to 262143 packet/sec, zero means no limit. The maximum available value of Fast Ethernet interface is 148810, this is the maximum packet number of the 100M throughput.

Enter the Rate field of the port you want assign, type in the new value and then press on the Enter key first. After assigned or changed the value on all the ports you want to configure. Click on **Apply** to apply the configuration of all ports. The Apply command applied all the ports' storm control value.

4.3.5 Port Trunking

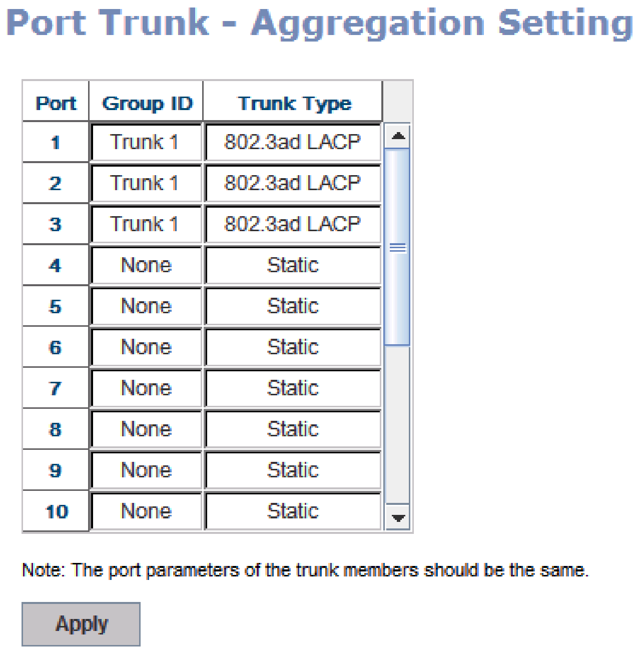
Port Trunking configuration allows you to group multiple Ethernet ports in parallel and to increase link bandwidth. The aggregated ports can be viewed as one physical port so that the bandwidth is higher than merely one single Ethernet port. The member ports of the same trunk group can balance the loading and backup for each other. Port Trunking feature is usually used when you need higher bandwidth for backbone network. This is an inexpensive way for you to transfer more data.

There are some different descriptions for the port trunking. Different manufacturers may use different descriptions for their products, like Link Aggregation Group (LAG), Link Aggregation Control Protocol, Ethernet Trunk, Ether Channel…etc. Most of the implementations now conform to IEEE standard, 802.3ad.

The aggregated ports can interconnect to the other switch which also supports Port Trunking. The switch supports 2 types of port trunking. One is Static Trunk, the other is 802.3ad. When the other end uses 802.3ad LACP, you **should** assign 802.3ad LACP to the trunk. When the other end uses non-802.3ad, you can then use Static Trunk. **In practical, the Static Trunk is suggested.**

There are two configuration pages, Aggregation Setting and Aggregation Status.

Aggregation Setting



Port Trunk - Aggregation Setting

Port	Group ID	Trunk Type
1	Trunk 1	802.3ad LACP
2	Trunk 1	802.3ad LACP
3	Trunk 1	802.3ad LACP
4	None	Static
5	None	Static
6	None	Static
7	None	Static
8	None	Static
9	None	Static
10	None	Static

Note: The port parameters of the trunk members should be the same.

Trunk Size: The switch can support up to 8 trunk groups. Each trunk group can support up to 8 member ports. Since the member ports should use same speed/duplex, the maximum trunk size is decided by the port volume.

Group ID: Group ID is the ID for the port trunking group. Ports with same group ID are in the same group. Click None, you can select the Trunk ID from Trunk 1 to Trunk 8.

Trunk Type: Static and **802.3ad LACP:** Each Trunk Group can only support Static or 802.3ad LACP. Choose the type you need here.

Extended setting in CLI

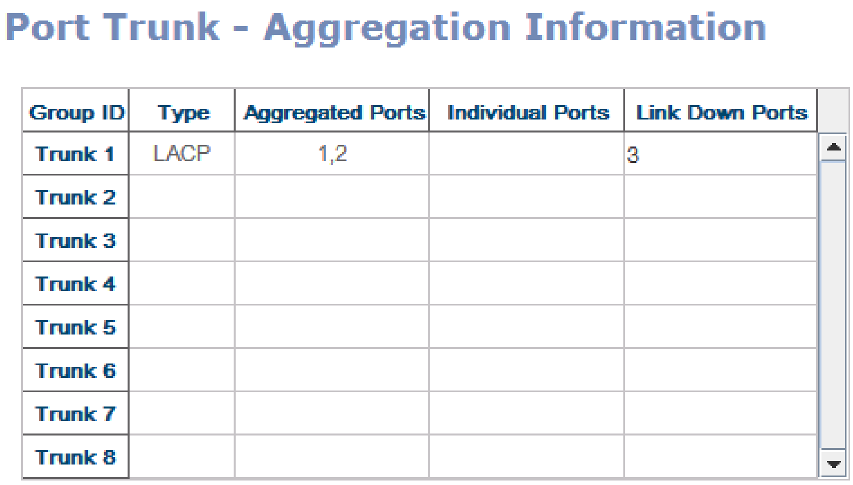
Port Priority: The command allows you to change the port priority setting on a specific port. LACP port priority is configured on each port using LACP and the port priority can be configured through the CLI. The priority is based on the higher number, the lower the priority and the default value is 32768.

LACP Timeout: The LACPDU is generated and continue transmit within the LACP group and the interval time of the LACPDU Long timeout is 30 sec which is a default setting. The LACPDP Short timeout is 1 sec, the command to change from Long to Short is only supported in the CLI If LACP port doesn't receive the any LACPDP packets 3 times, the port may leave the group without earlier inform or is not detected by the switch, then the port will be removed from the group.

This command can be used when connect the switch by 2-port LACP through not-direct connected or shared media. The end of the switch may not directly detect the failure; the LACP Short Timeout can detect the LACP group failure earlier within 3 seconds.

Aggregation Status

This page shows the status of port aggregation. Once the aggregation ports are established, you will see following status.



Port Trunk - Aggregation Information

Group ID	Type	Aggregated Ports	Individual Ports	Link Down Ports
Trunk 1	LACP	1,2		3
Trunk 2				
Trunk 3				
Trunk 4				
Trunk 5				
Trunk 6				
Trunk 7				
Trunk 8				

Group ID: Display Trunk 1 to Trunk 8 set up in Aggregation Setting.

Type: Static or LACP set up in Aggregation Setting.

Aggregated: When the LACP links is up, you can see the member ports in Aggregated column.

Individual: When LACP is enabled, member ports of LACP group which are not connected to correct LACP member ports will be displayed in the Individual column.

Link Down: When LACP is enabled, member ports of LACP group which are not linked up will be displayed in the Link Down column.

4.3.6 Command Lines for Port Configuration

Feature	Command Line
Port Control	
Port Control – State	Switch(config-if)# shutdown -> Disable port state interface fastethernet1 is shutdown now. Switch(config-if)# no shutdown -> Enable port state interface fastethernet1 is up now.
Port Control – Auto Negotiation	Switch(config)# interface fa1 Switch(config-if)# auto-negotiation Auto-negotiation of port 1 is enabled!

Port Control – Force Speed/Duplex	Switch(config-if)# speed 100 set the speed mode ok! Switch(config-if)# duplex full set the duplex mode ok!
Port Control – Flow Control	Switch(config-if)# flowcontrol on Flowcontrol on for port 1 set ok! Switch(config-if)# flowcontrol off Flowcontrol off for port 1 set ok!
Port Status	

Port Status	Switch# show interface fa1
	Interface fastethernet1
	    Administrative Status : Enable
	    Operating Status : Connected
	    Duplex : Full
	    Speed : 100
	    MTU: 1518
	    Flow Control :off
	    Default Port VLAN ID: 1
	    Ingress Filtering : Disabled
	    Acceptable Frame Type : All
	    Port Security : Disabled
	    Auto Negotiation : Disable
	    Loopback Mode : None
	    STP Status: forwarding
	    Default CoS Value for untagged packets is 0.
	    Mdix mode is Disable.
	    Medium mode is Copper.
	
	Note: Administrative Status -> Port state of the port. Operating status -> Current status of the port. Duplex -> Duplex mode of the port. Speed -> Speed mode of the port. Flow control -> Flow Control status of the port.

Rate Control	
Rate Control – Ingress or Egress	Switch(config-if)# rate-limit egress Outgoing packets ingress Incoming packets ***Note: To enable rate control, you should select the Ingress or Egress rule first; then assign the packet type and bandwidth.***
Rate Control - Bandwidth	Switch(config-if)# rate-limit ingress bandwidth <0-1000000> Limit in kilobits per second (FE: 0-100000, GE: 0-1000000, 0 is no limit) Switch(config-if)# rate-limit ingress bandwidth 800 Set the ingress rate limit 800Kbps for Port 1..
Storm Control	

Strom Control – Rate Configuration (Packet Type)	Switch(config-if)# storm-control
	broadcast Broadcast packets
	dlf Destination Lookup Failure
	multicast Multicast packets
	
	SWITCH(config)# storm-control broadcast ?
	<0-100000> Rate limit value 0~100000Kbyte/sec
	SWITCH(config)# storm-control broadcast 10000
	limit_rate = 10000
	Set rate limit for Broadcast packets.
	SWITCH(config)# storm-control multicast 1000
	limit_rate = 1000
	Set rate limit for Multicast packets.
	SWITCH(config)# storm-control dlf 1000
	limit_rate = 1000
	Set rate limit for Destination Lookup Failure packets.

Storm Control - Enable Storm Control to a port	SWITCH(config)# interface fa1 SWITCH(config-if)# storm-control broadcast Broadcast packets dlf Destination Lookup Failure multicast Multicast packets SWITCH(config-if)# storm-control broadcast <cr> SWITCH(config-if)# storm-control broadcast

	Enables rate limit for Broadcast packets for Port 1. (Continue apply to other ports)
Display – Rate Configuration and port status	SWITCH# show storm-control Storm-control rate limit: DLF:1000(Kbytes/sec) Multicast:1000(Kbytes/sec) Broadcast:1000(Kbytes/sec) -- Port 1: DLF Enable Broadcast Enable Multicast Enable Port 2: DLF Enable Broadcast Enable Multicast Enable …………
Port Trunking	
LACP	Switch(config)# lacp group 1 gi8-10 Group 1 based on LACP(802.3ad) is enabled! *Note: The interface list is fa1,fa3-5, gi8-10* Note: different speed port can’t be aggregated together.
LACP – Port Setting	SWITCH(config-if)# lacp port-priority LACP priority for physical interfaces timeout assigns an administrative LACP timeout SWITCH(config-if)# lacp port-priority <1-65535> Valid port priority range 1 - 65535 (default is 32768) SWITCH(config-if)# lacp timeout long specifies a long timeout value (default) short specifies a short timeout value SWITCH(config-if)# lacp timeout short Set lacp port timeout ok.

Static Trunk	Switch(config)# trunk group 2 fa6-7 Trunk group 2 enable ok! Failure to configure due to the group ID is existed. SWITCH(config)# trunk group 1 fa11-12 Can't set trunk group 1 enable! The group 1 is a lacp enabled group! SWITCH(config)# trunk group 2 fa11-12 Can't set trunk group 2 enable! The group 2 is a static aggregation group.
Display - LACP	Switch# show lacp counters LACP statistical information group LACP group internal LACP internal information neighbor LACP neighbor information port-setting LACP setting for physical interfaces system-id LACP system identification system-priority LACP system priority SWITCH# show lacp port-setting LACP Port Setting : Port Priority Timeout ----- --------- -------- 1 32768 Long 2 32768 Long 3 32768 Long ………. Switch# show lacp internal LACP group 1 internal information: LACP Port Admin Oper Port Port Priority Key Key State ----- ----------- -------- -------- ------- 8 1 8 8 0x45 9 1 9 9 0x45 10 1 10 10 0x45

	LACP group 2 is inactive LACP group 3 is inactive LACP group 4 is inactive
Display - Trunk	Switch# show trunk group 1 FLAGS: I -> Individual P -> In channel D -> Port Down Trunk Group GroupID Protocol Ports --------+---------+------------------------------------ 1 LACP 8(D) 9(D) 10(D)

4.4 Network Redundancy

The switch firmware supports standard RSTP, MSTP, Multiple Super Ring, Rapid Dual Homing.

MDI-128-F4G Series support advanced Multiple Spanning Tree Protocol (MSTP). This protocol is a direct extension of RSTP. It can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group (as sometimes occurs with IEEE 802.1D STP).

Multiple Super Ring (MSR) technology, 0 milliseconds for restore and less than 300 milliseconds for failover.

Advanced Rapid Dual Homing (RDH) technology also facilitates the switch to connect with a core managed switch easily and conveniently. With RDH technology, you can also group several Rapid Super Rings or RSTP cloud together, which is also known as Auto Ring Coupling.

Besides ring technology, the switch also supports 802.1D-2004 version Rapid Spanning Tree Protocol (RSTP). New version of RSTP standard includes 802.1D-1998 STP, 802.1w RSTP.

Following commands are included in this section:

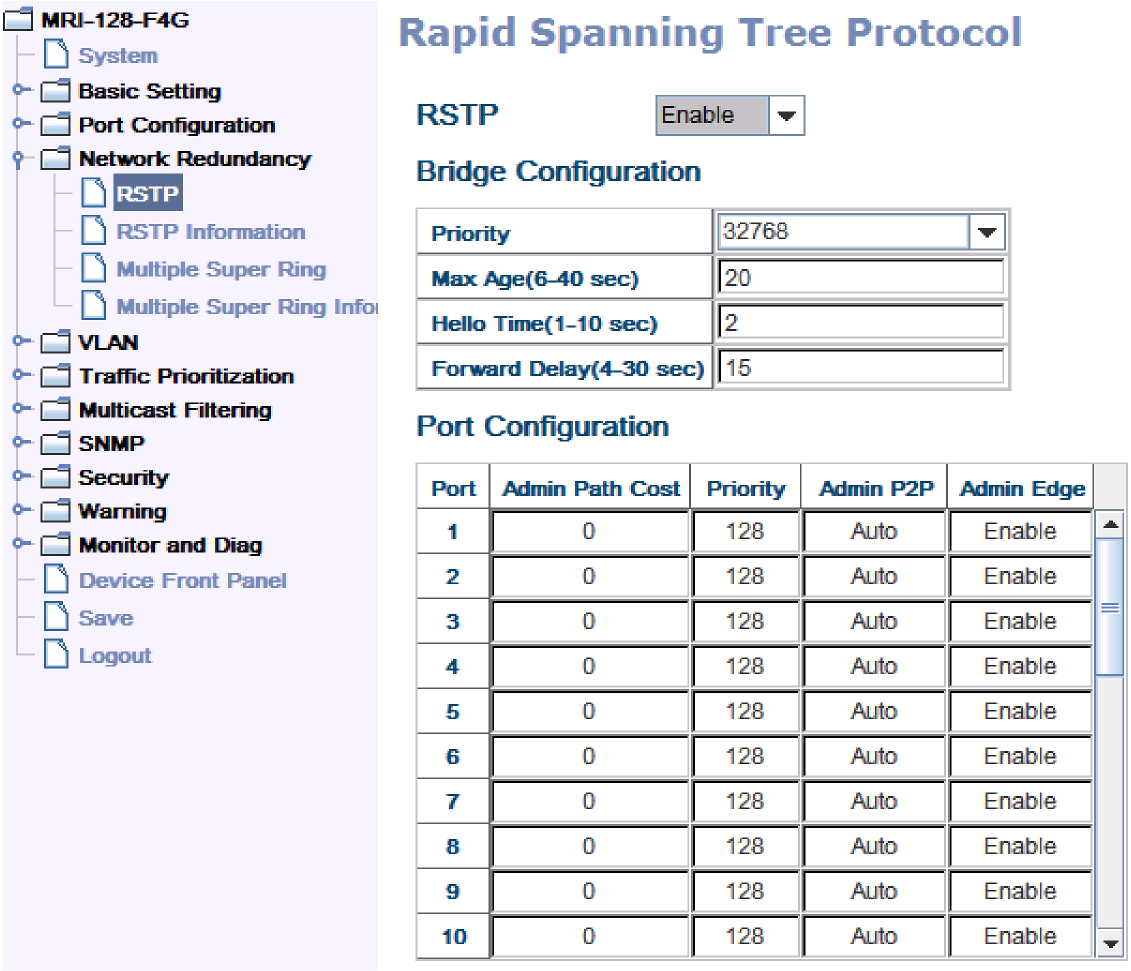
4.4.1 RSTP
4.4.2 RSTP Info
4.4.3 MSTP
4.4.4 MSTP Info
4.4.5 Multiple Super Ring
4.4.6 Ring Info
4.4.7 Command Lines for Network Redundancy

4.4.1 RSTP

RSTP is the abbreviation of Rapid Spanning Tree Protocol. If a switch has more than one path to a destination, it will lead to message loops that can generate broadcast storms and quickly bog down a network. The spanning tree was created to combat the negative effects of message loops in switched networks. A spanning tree uses a spanning tree algorithm (STA) to automatically sense whether a switch has more than one way to communicate with a node. It will then select the best path (primary), and block the other path(s). It will also keep track of the blocked path(s) in case the primary path fails. Spanning Tree Protocol

(STP) introduced a standard method to accomplish this. It is specified in IEEE 802.1D-1998. Later, Rapid Spanning Tree Protocol (RSTP) was adopted and represents the evolution of STP, providing much faster spanning tree convergence after a topology change. This is specified in IEEE 802.1w. In 2004, 802.1w is included into 802.1D-2004 version. This switch supports both RSTP and STP (all switches that support RSTP are also backward compatible with switches that support only STP).

This page allows you to enable/disable RSTP, configure the global setting and port settings.



Rapid Spanning Tree Protocol

RSTP: Enable

Bridge Configuration

Priority	32768
Max Age(6-40 sec)	20
Hello Time(1-10 sec)	2
Forward Delay(4-30 sec)	15

Port Configuration

Port	Admin Path Cost	Priority	Admin P2P	Admin Edge
1	0	128	Auto	Enable
2	0	128	Auto	Enable
3	0	128	Auto	Enable
4	0	128	Auto	Enable
5	0	128	Auto	Enable
6	0	128	Auto	Enable
7	0	128	Auto	Enable
8	0	128	Auto	Enable
9	0	128	Auto	Enable
10	0	128	Auto	Enable

<u>**RSTP Mode**</u>: You must first enable STP/RSTP mode, before configuring any related parameters. Parameter settings required for both STP and RSTP are the same. Note that 802.1d refers to STP mode, while 802.1w refers to faster RSTP mode.

<u>**Bridge Configuration**</u>

Priority (0-61440): RSTP uses bridge ID to determine the root bridge, the bridge with the highest bridge ID becomes the root bridge. The bridge ID is composed of bridge priority and bridge MAC address. So that the bridge with the highest priority becomes the highest bridge ID. If all the bridge ID has the same priority, the bridge with the lowest MAC address will then become the root bridge.

Note: The bridge priority value must be in multiples of 4096. A device with a lower number has a higher bridge priority. Ex: 4096 is higher than 32768.

Max Age (6-40): Enter a value from 6 to 40 seconds here. This value represents the time that a bridge will wait without receiving Spanning Tree Protocol configuration messages before attempting to reconfigure.

If the switch is not the root bridge, and if it has not received a hello message from the root bridge in an amount of time equal to Max Age, then Switch will reconfigure itself as a root bridge. Once two or more devices on the network are recognized as a root bridge, the devices will renegotiate to set up a new spanning tree topology.

The MAX Age value affects the maximum volume of the RSTP loop. In the RSTP BPDU packet, there is one field, message age which start from 0, add 1 after passed one hop in the RSTP loop. When the message age is larger than MAX Age, the BPDU would be ignored and the lower switches are separated to different RSTP domain. The switches in other RSTP domain can’t be managed through upper switch.

Since different RSTP aware switches may have their own mechanism to calculate the message age. So that this is most possibly occurred when interoperate different vendors’ RSTP aware switches together. The maximum volume of the RSTP domain is 23, configure the MAX Age lower than 23 is recommended.

Hello Time (1-10): Enter a value from 1 to 10 seconds here. This is a periodic timer that drives the switch to send out BPDU (Bridge Protocol Data Unit) packet to check current STP status.

The root bridge of the spanning tree topology periodically sends out a “hello” message to other devices on the network to check if the topology is “healthy”. The “hello time” is the amount of time the root has waited during sending hello messages.

Forward Delay Time (4-30): Enter a value between 4 and 30 seconds. This value is the time that a port waits before changing from Spanning Tree Protocol learning and listening states to forwarding state.

This is the amount of time Switch will wait before checking to see if it should be changed to a different state.

Once you have completed your configuration, click on **Apply** to apply your settings.

Note: You must observe the following rule to configure Hello Time, Forwarding Delay, and Max Age parameters.

2 × (Forward Delay Time – 1 sec) ≥ Max Age Time ≥ 2 × (Hello Time value + 1 sec)

Port Configuration

Select the port you want to configure and you will be able to view current settings and status of the port.

Path Cost: Enter a number between 1 and 200,000,000. This value represents the "cost" of the path to the other bridge from the transmitting bridge at the specified port.

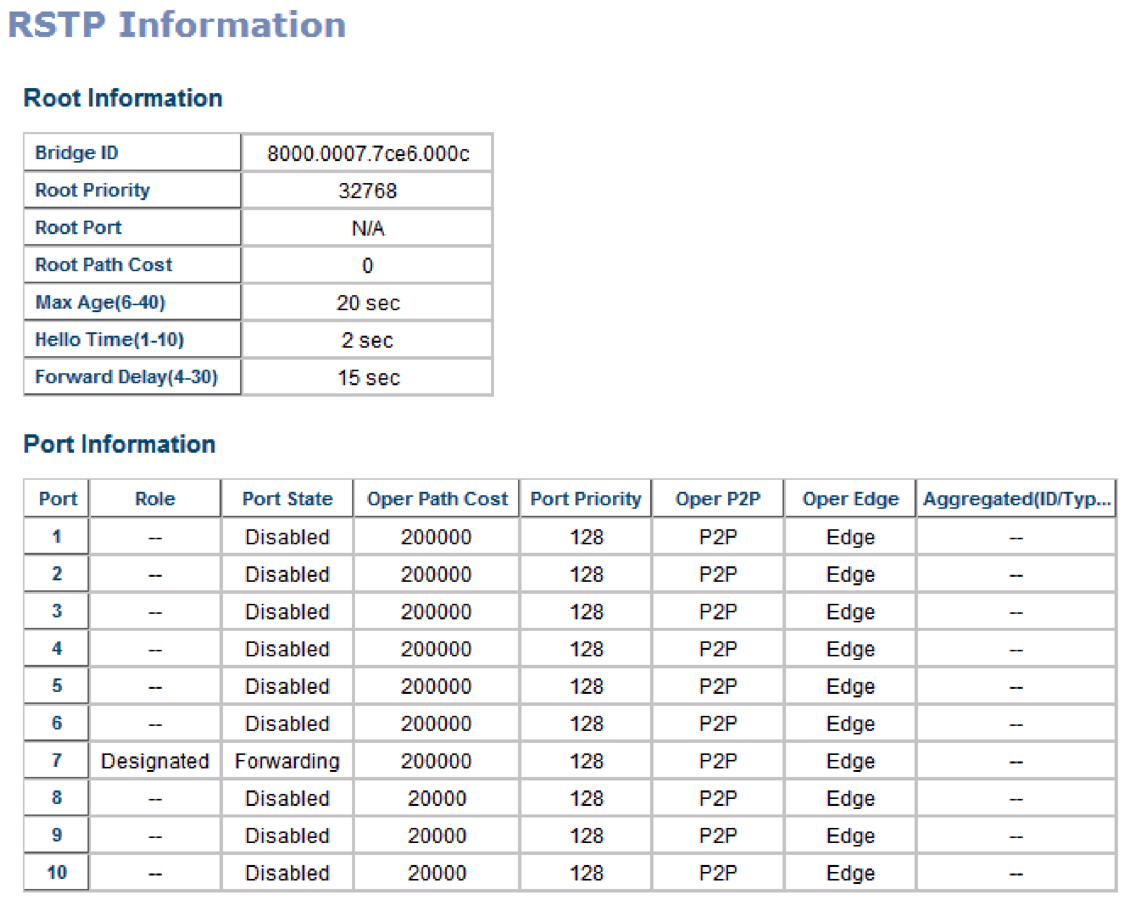
Priority: Enter a value between 0 and 240, using multiples of 16. This is the value that decides which port should be blocked by priority in a LAN.

Admin P2P: Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to another bridge (i.e. it is served by a point-to-point LAN segment), or if it can be connected to two or more bridges (i.e. it is served by a shared-medium LAN segment). This function allows P2P status of the link to be manipulated administratively. "**Auto**" means to auto select P2P or Share mode. "**P2P"** means P2P is enabled, while "**Share"** means P2P is disabled.

Admin Edge: A port directly connected to the end stations cannot create a bridging loop in the network. To configure this port as an edge port, set the port to the **Enable** state. When the non-bridge device connects an admin edge port, this port will be in blocking state and turn to forwarding state in 4 seconds.

Once you finish your configuration, click on **Apply** to save your settings.

4.4.2 RSTP Info



RSTP Information

Root Information

Bridge ID	8000.0007.7ce6.000c
Root Priority	32768
Root Port	N/A
Root Path Cost	0
Max Age(6-40)	20 sec
Hello Time(1-10)	2 sec
Forward Delay(4-30)	15 sec

Port Information

Port	Role	Port State	Oper Path Cost	Port Priority	Oper P2P	Oper Edge	Aggregated(ID/Typ...
1	--	Disabled	200000	128	P2P	Edge	--
2	--	Disabled	200000	128	P2P	Edge	--
3	--	Disabled	200000	128	P2P	Edge	--
4	--	Disabled	200000	128	P2P	Edge	--
5	--	Disabled	200000	128	P2P	Edge	--
6	--	Disabled	200000	128	P2P	Edge	--
7	Designated	Forwarding	200000	128	P2P	Edge	--
8	--	Disabled	20000	128	P2P	Edge	--
9	--	Disabled	20000	128	P2P	Edge	--
10	--	Disabled	20000	128	P2P	Edge	--

This page allows you to see the information of the root switch and port status.

Root Information: You can see root Bridge ID, Root Priority, Root Port, Root Path Cost and the Max Age, Hello Time and Forward Delay of BPDU sent from the root switch.

Port Information: You can see port Role, Port State, Path Cost, Port Priority, Oper P2P mode, Oper edge port mode and Aggregated(ID/Type).

4.4.3 MSTP (Multiple Spanning Tree Protocol) Configuration

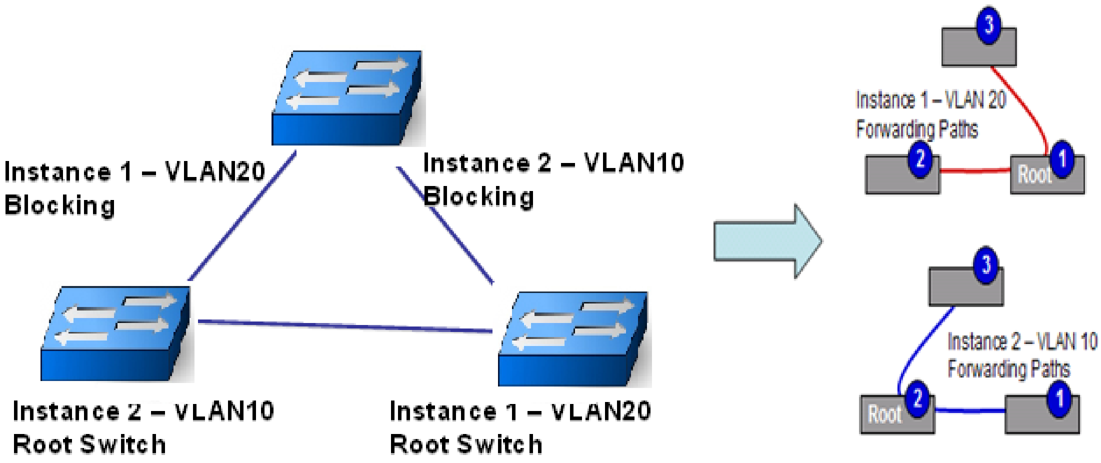
MSTP is the abbreviation of Multiple Spanning Tree Protocol. This protocol is a direct extension of RSTP. It can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group (as sometimes occurs with IEEE 802.1D STP).

While using MSTP, there are some new concepts of network architecture. A switch may belong to different groups, act as root or designate switch, generate BPDU for the network to maintain the forwarding table of the spanning tree.

With MSTP can also provide multiple forwarding paths and enable load balancing. Understand the architecture allows you to maintain the correct spanning tree and operate effectively.

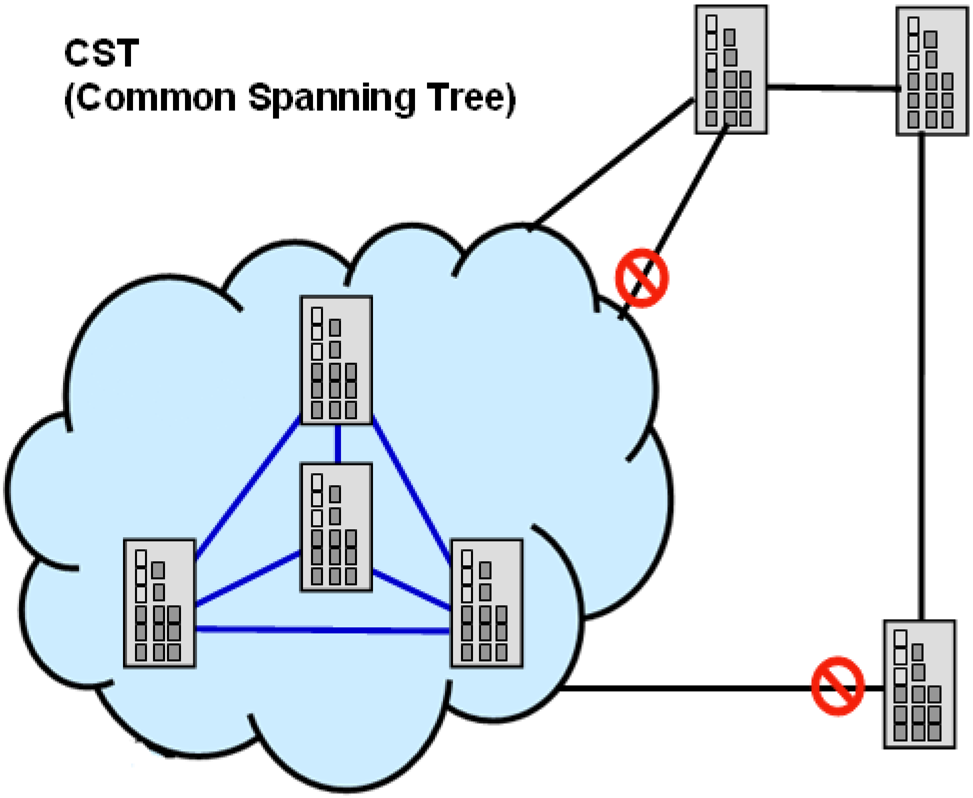
One VLAN can be mapped to a Multiple Spanning Tree Instance (MSTI). For example, the maximum Instance switch support is usually 16, range from 0-15. The MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. An Internal Spanning Tree (IST) is used to connect all the MSTP switches within an MST region. An MST Region may contain multiple MSTP Instances.

The figure shows there are 2 VLANs/MSTP Instances and each instance has its Root and forwarding paths.

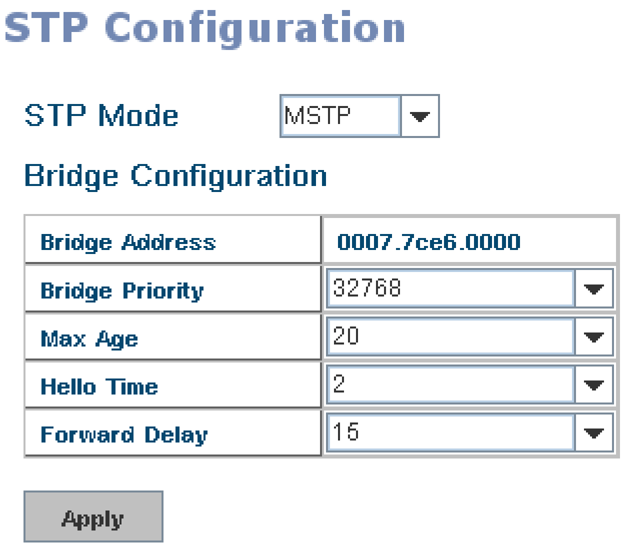


A Common Spanning Tree (CST) interconnects all adjacent MST regions and acts as a virtual bridge node for communications with STP or RSTP nodes in the global network. MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between switches that support the STP, RSTP, MSTP protocols.

The figure shows the CST large network. In this network, a Region may has different instances and its own forwarding path and table, however, it acts as a single Brige of CST.



To configure the MSTP setting, the STP Mode of the STP Configuration page should be changed to MSTP mode first.



STP Configuration

STP Mode: MSTP

Bridge Configuration

Bridge Address	0007.7ce6.0000
Bridge Priority	32768
Max Age	20
Hello Time	2
Forward Delay	15

After enabled MSTP mode, then you can go to the MSTP Configuration pages.

MSTP Region Configuration

This page allows configure the Region Name and its Revision, mapping the VLAN to Instance and check current MST Instance configuration. The network can be divided virtually to different Regions. The switches within the Region should have the same Region and Revision level.

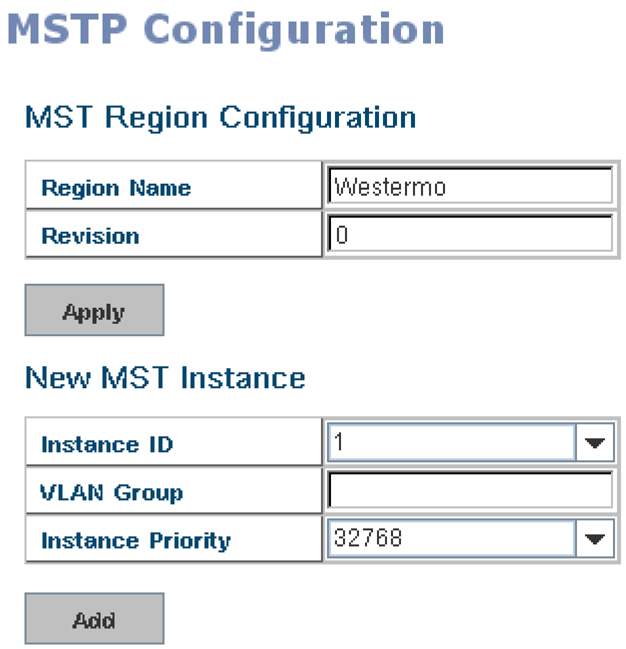
Region Name: The name for the Region. Maximum length: 32 characters.

Revision: The revision for the Region. Range: 0-65535; Default: 0)

Once you finish your configuration, click on **Apply** to apply your settings.

New MST Instance

This page allows mapping the VLAN to Instance and assign priority to the instance. Before mapping VLAN to Instance, you should create VLAN and assign the member ports first. Please refer to the VLAN setting page.



MSTP Configuration

MST Region Configuration

Region Name	Westermo
Revision	0

New MST Instance

Instance ID	1
VLAN Group	
Instance Priority	32768

Instance ID: Select the Instance ID, the available number is 1-15.

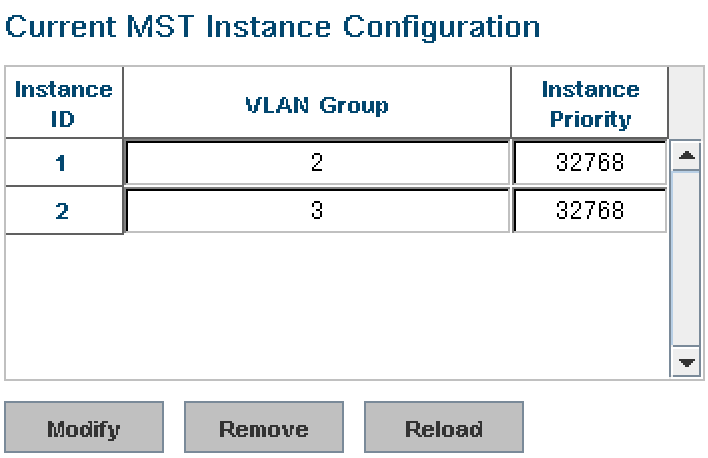
VLAN Group: Type the VLAN ID you want mapping to the instance.

Instance Priority: Assign the priority to the instance.

After finish your configuration, click on **Add** to apply your settings.

Current MST Instance Configuration

This page allows you to see the current MST Instance Configuration you added. Click on “**Apply**” to apply the setting. You can “**Remove”** the instance or “**Reload**“ the configuration display in this page.



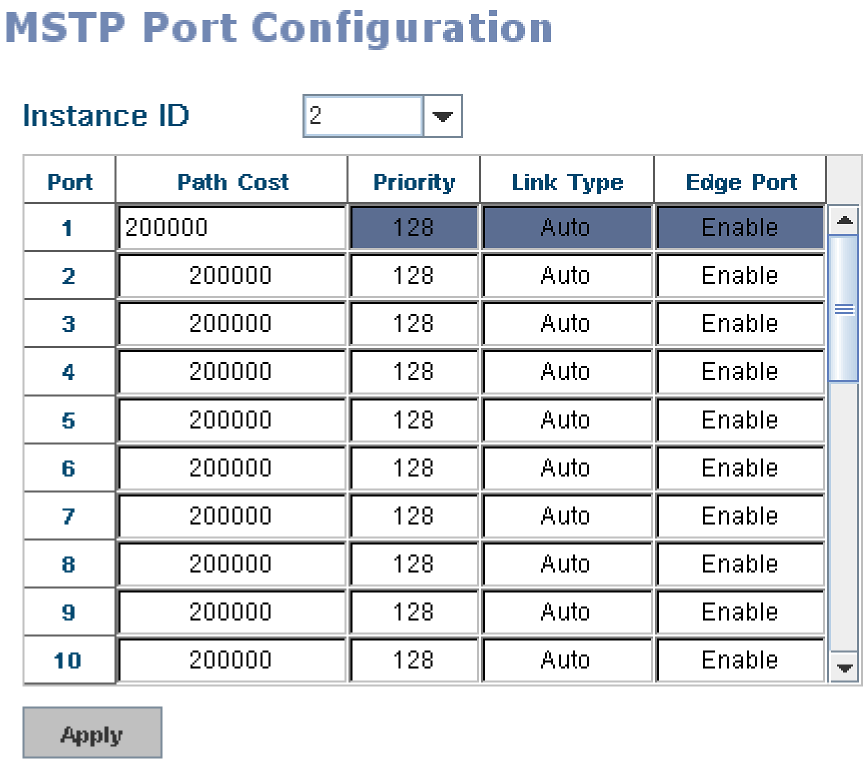
Current MST Instance Configuration

Instance ID	VLAN Group	Instance Priority
1	2	32768
2	3	32768

MSTP Port Configuration

This page allows configure the Port settings. Choose the Instance ID you want to configure. The MSTP enabled and linked up ports within the instance will be listed in this table.

Note that the ports not belonged to the Instance, or the ports not MSTP activated will not display. The meaning of the Path Cost, Priority, Link Type and Edge Port is the same as the definition of RSTP.



MSTP Port Configuration

Instance ID: 2

Port	Path Cost	Priority	Link Type	Edge Port
1	200000	128	Auto	Enable
2	200000	128	Auto	Enable
3	200000	128	Auto	Enable
4	200000	128	Auto	Enable
5	200000	128	Auto	Enable
6	200000	128	Auto	Enable
7	200000	128	Auto	Enable
8	200000	128	Auto	Enable
9	200000	128	Auto	Enable
10	200000	128	Auto	Enable

Path Cost: Enter a number between 1 and 200,000,000. This value represents the "cost" of the path to the other bridge from the transmitting bridge at the specified port.

Priority: Enter a value between 0 and 240, using multiples of 16. This is the value that decides which port should be blocked by priority in a LAN.

Link Type: There are 3 types for you select. **Auto, P2P** and **Share.**

Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to another bridge (i.e. it is served by a point-to-point LAN segment), or if it can be connected to two or more bridges (i.e. it is served by a shared-medium LAN segment). This function allows link status of the link to be manipulated administratively. "**Auto**" means to auto select P2P or Share mode. "**P2P"** means P2P is enabled, the 2 ends work in Full duplex mode. While "**Share"** is enabled, it means P2P is disabled, the 2 ends may connect through a share media and work in Half duplex mode.

Edge: A port directly connected to the end stations cannot create a bridging loop in the network. To configure this port as an edge port, set the port to the **Enable** state. When the non-bridge device connects an admin edge port, this port will be in blocking state and turn to forwarding state in 4 seconds.

Once you finish your configuration, click on **Apply** to save your settings.

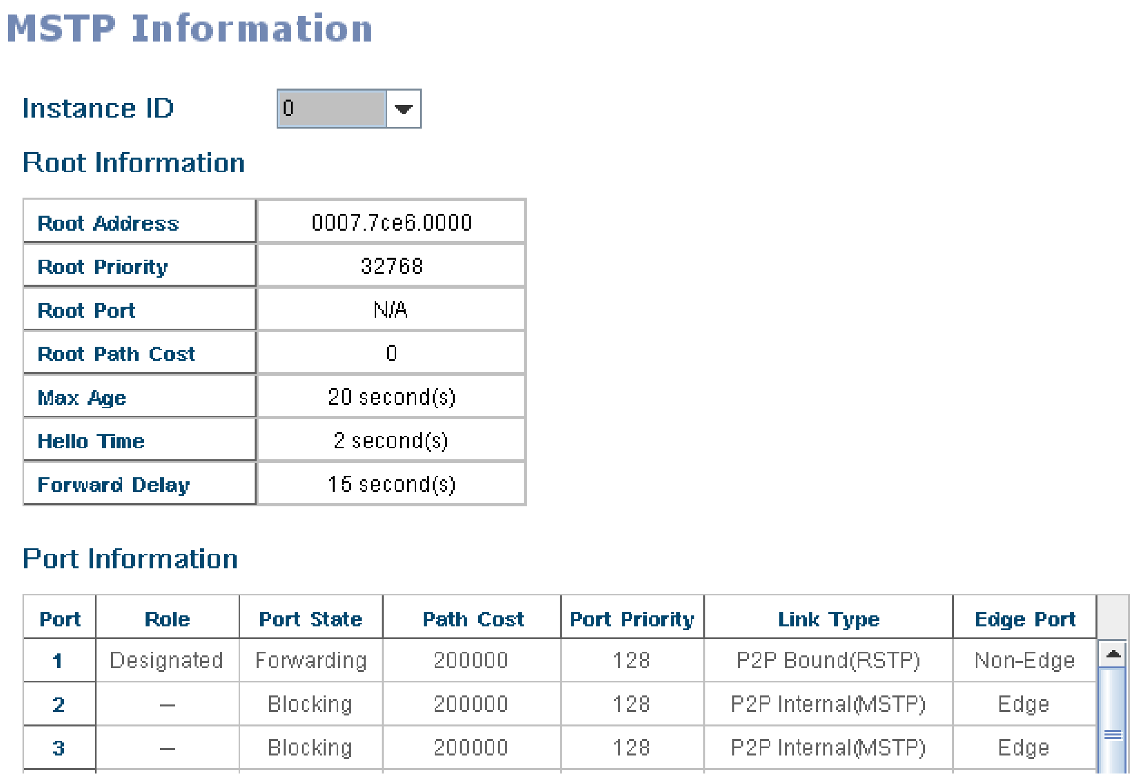
4.4.4 MSTP Information

This page allows you to see the current MSTP information.

Choose the **Instance ID** first. If the instance is not added, the information remains blank.

The **Root Information** shows the setting of the Root switch.

The **Port Information** shows the port setting and status of the ports within the instance.



MSTP Information

Instance ID: 0

Root Information

Root Address	0007.7ce6.0000
Root Priority	32768
Root Port	N/A
Root Path Cost	0
Max Age	20 second(s)
Hello Time	2 second(s)
Forward Delay	15 second(s)

Port Information

Port	Role	Port State	Path Cost	Port Priority	Link Type	Edge Port
1	Designated	Forwarding	200000	128	P2P Bound(RSTP)	Non-Edge
2	–	Blocking	200000	128	P2P Internal(MSTP)	Edge
3	–	Blocking	200000	128	P2P Internal(MSTP)	Edge

Click on “**Reload**“ to reload the MSTP information display.

4.4.5 Multiple Super Ring (MSR)

The most common industrial network redundancy is to form a ring or loop. Typically, the managed switches are connected in series and the last switch is connected back to the first one.

The Multiple Super Ring has enhanced Ring Master selection and faster recovery time. It is also enhanced for more complex ring application.

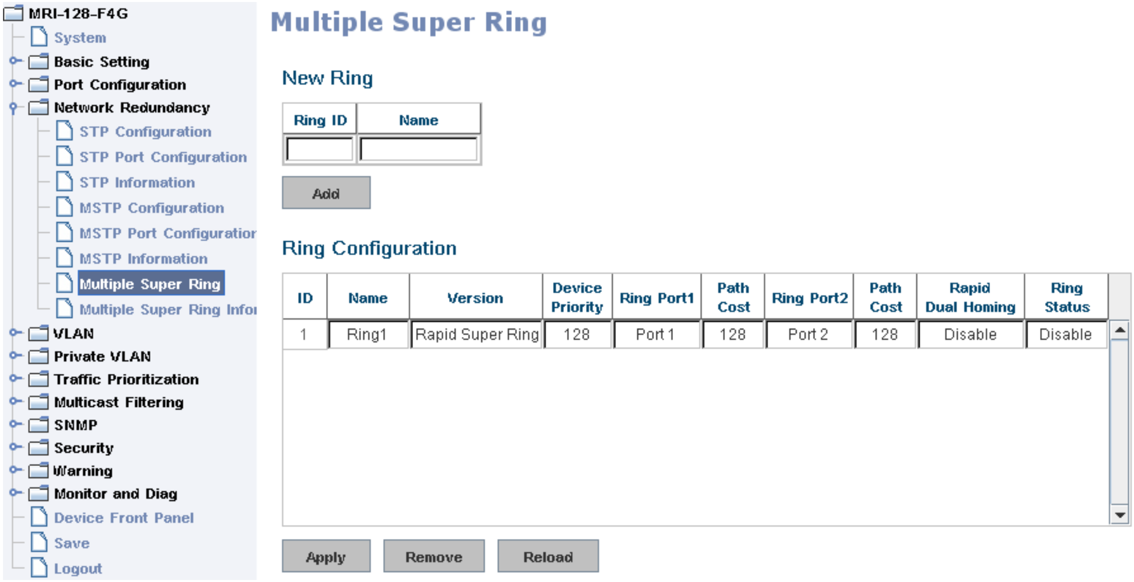
Multiple Super Ring (MSR) technology have a fast restore and failover time in the world, 0 ms for restore and less than 300 ms for failover. Advanced **Rapid Dual Homing (RDH)** technology also facilitates Managed Switch to connect with a core managed switch easily and conveniently. With RDH technology, you can also couple several Rapid Super Rings or RSTP cloud together, which is also known as Auto Ring Coupling.

TrunkRing technology allows integrate MSR with LACP/Port Trunking. The LACP/Trunk aggregated ports is a virtual interface and it can work as the Ring port of the MSR.

MultiRing is an outstanding technology that multiple rings can be aggregated within one switch by using different Ring ID. The maximum Ring number one switch can support is half of total port volume. For example, the switch is a 24+4G port design, which means 12 x 100M Rings and 2 Gigabit Rings can be aggregated to one the switch. The feature saves much effort when constructing complex network architecture.

This page allows you to enable the settings for Multiple Super Ring and Rapid Dual Homing.

New Ring: To create a Rapids Super Ring. Just fill in the Ring ID which has range from 0 to 31. If the name field is left blank, the names of this ring will automatically be naming with the Ring ID.



Multiple Super Ring

New Ring

Ring ID	Name

Ring Configuration

ID	Name	Version	Device Priority	Ring Port1	Path Cost	Ring Port2	Path Cost	Rapid Dual Homing	Ring Status
1	Ring1	Rapid Super Ring	128	Port 1	128	Port 2	128	Disable	Disable

<u>**Ring Configuration**</u>

<u>**ID:**</u> Once a Ring is created, it appears and cannot be changed. In multiple rings' environment, the traffic can only be forwarded under the same ring ID.

<u>**Name:**</u> This field will show the name of the Ring. If it is not filled in when creating, it will be automatically named by the rule "RingID".

<u>**Version:**</u> The version of Ring can be changed here. There are three modes to choose: Rapid Super Ring as default.

<u>**Device Priority:**</u> The switch with highest priority (highest value) will be automatically selected as Ring Master. Then one of the ring ports in this switch will become forwarding port and the other one will become blocking port. If all of the switches have the same priority, the switch with the biggest MAC address will be selected as Ring Master.

Ring Port1: In Rapid Super Ring environment, you should have two Ring Ports. No matter this switch is Ring Master or not, when configuring RSR, two ports should be selected to be Ring Ports. For Ring Master, one of the ring ports will become the forwarding port and the other one will become the blocking port.

Path Cost: Change the Path Cost of Ring Port1. If this switch is the Ring Master of a Ring, then it determines the blocking port. The Port with higher Path Cost in the two rings Port will become the blocking port, if the Path Cost is the same, the port with larger port number will become the blocking port.

Ring Port2: Assign another port for ring connection

Path Cost: Change the Path Cost of Ring Port2

Rapid Dual Homing: Rapid Dual Homing is a feature of MSR. When you want to connect multiple RSR or form a redundant topology with other vendors, RDH could allow you to have maximum seven multiple links for redundancy without any problem.

In Rapid Dual Homing, you don’t need to configure specific port to connect to other protocol. The Rapid Dual Homing will smartly choose the fastest link for primary link and block all the other links to avoid loop. If the primary link failed, Rapid Dual Homing will automatically forward the secondary link for network redundancy. If there are more connections, they will be standby links and recover one of them if both primary and secondary links are down.

Ring status: To enable/disable the Ring. Please remember to enable the ring after you add it.

MultiRing: The MultiRing technology is one of the patterns of the MSR technology; the technology allows you to aggregate multiple rings within one switch. Create multiple ring ID and assign different ring port 1 and port 2 to each ring, thus the switch can have multiple rings in one switch.

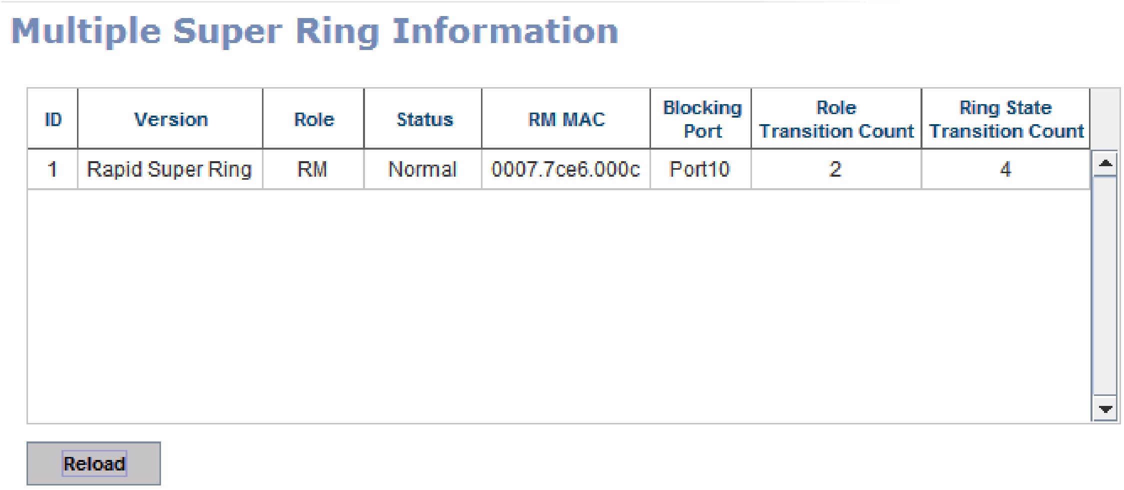
When implementing MultiRing, remember that the different rings can NOT use the same ring ID. The other settings are the same as above description.

Technically, the maximum ring volume the MultiRing supported is up to 16 rings. Due to the port volume limitation, the maximum value is half of the port volume of a switch.

TrunkRing: The MultiRing technology is part of the MSR technology which combines the MSR with the port trunking technology. After multiple ports aggregated, this is so-call port trunking (Static or learnt by LACP protocol), the Trunk ID can be one of the port ID of the MSR technology. Configured the port trunking first then you can add the Trunk group as a Ring Port in managed switch.

4.4.6 Ring Info

This page shows the MSR information.



Multiple Super Ring Information

ID	Version	Role	Status	RM MAC	Blocking Port	Role Transition Count	Ring State Transition Count
1	Rapid Super Ring	RM	Normal	0007.7ce6.000c	Port10	2	4

ID: Ring ID.

Version: which version of this ring.

Role: This Switch is RM or nonRM

Status: If this field is Normal which means the redundancy is activated. If any one of the links in the ring is down, then the status will be Abnormal.

RM MAC: The MAC address of Ring Master of this Ring. It helps to find the redundant path.

Blocking Port: This field shows which is blocked port of RM.

Role Transition Count: This shows how many times this switch has changed its Role from nonRM to RM or from RM to nonRM.

Role state Transition Count: This number shows how many times the Ring status has been transformed between Normal and Abnormal state.

4.4.7 Command Lines:

Feature	Command Line
Global	
Enable	Switch(config)# spanning-tree enable
Disable	Switch (config)# spanning-tree disable
Mode (Choose the Spanning Tree mode)	Switch(config)# spanning-tree mode rst the rapid spanning-tree protocol (802.1w) stp the spanning-tree prtotcol (802.1d) mst the multiple spanning-tree protocol (802.1s)
Bridge Priority	Switch(config)# spanning-tree priority <0-61440> valid range is 0 to 61440 in multiple of 4096 Switch(config)# spanning-tree priority 4096

Bridge Times	Switch(config)# spanning-tree bridge-times (forward Delay) (max-age) (Hello Time) Switch(config)# spanning-tree bridge-times 15 20 2 This command allows you configure all the timing in one time.
Forward Delay	Switch(config)# spanning-tree forward-time <4-30> Valid range is 4~30 seconds Switch(config)# spanning-tree forward-time 15
Max Age	Switch(config)# spanning-tree max-age <6-40> Valid range is 6~40 seconds Switch(config)# spanning-tree max-age 20
Hello Time	Switch(config)# spanning-tree hello-time <1-10> Valid range is 1~10 seconds Switch(config)# spanning-tree hello-time 2
MSTP	
Enter the MSTP Configuration Tree	Switch(config)# spanning-tree mst MSTMAP the mst instance number or range configuration enter mst configuration mode forward-time the forwaoreneay time hello-time the hello time max-age the message maximum age time max-hops the maximum hops sync sync port state of exist vlan entry Switch(config)# spanning-tree mst configuration Switch(config)# spanning-tree mst configuration Switch(config-mst)# abort exit current mode and discard all changes end exit current mode, change to enable mode and apply all changes exit exit current mode and apply all changes instance the mst instance list Print command list name the name of mst region no Negate a command or set its defaults quit exit current mode and apply all changes revision the revision of mst region show show mst configuration

Region Configuration	Region Name: Switch(config-mst)# name NAME the name string Switch(config-mst)# naorenixnix Region Revision: Switch(config-mst)# revision <0-65535> the value of revision Switch(config-mst)# revision 65535
Mapping Instance to VLAN (Ex: Mapping VLAN 2 to Instance 1)	Switch(config-mst)# instance <1-15> target instance number Switch(config-mst)# instance 1 vlan VLANMAP target vlan number(ex.10) or range(ex.1-10) Switch(config-mst)# instance 1 vlan 2
Display Current MST Configuration	Switch(config-mst)# show current Current MST configuration Name orenixnix] Revision 65535 Instance Vlans Mapped -------- -------------------------------------- 0 1,4-4094 1 2 2 -- Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D --

Remove Region Name	Switch(config-mst)# no
	  name name configure
	  revision revision configure
	  instance the mst instance
	Switch(config-mst)# no name

Remove Instance example	Switch(config-mst)# no instance <1-15> target instance number Switch(config-mst)# no instance 2
Show Pending MST Configuration	Switch(config-mst)# show pending Pending MST configuration Name [] (->The name is removed by no name) Revision 65535 Instance Vlans Mapped -------- -------------------------------------- 0 1,3-4094 1 2 (->Instance 2 is removed by no instance --

	Config HMAC-MD5 Digest: 0x3AB68794D602FDF43B21C0B37AC3BCA8 ---
Apply the setting and go to the configuration mode	Switch(config-mst)# quit apply all mst configuration changes Switch(config)#
Apply the setting and go to the global mode	Switch(config-mst)# end apply all mst configuration changes Switch#
Abort the Setting and go to the configuration mode. Show Pending to see the new settings are not applied.	Switch(config-mst)# abort discard all mst configuration changes Switch(config)# spanning-tree mst configuration Switch(config-mst)# show pending Pending MST configuration Name orenixnix] (->The nameis not applied after Abort settings.) Revision 65535 Instance Vlans Mapped -------- ------------------------------------- 0 1,4-4094 1 2 2 3 (-> The instance is not applied after Abort settings-- Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D ---
RSTP	
The mode should be rst, the timings can be configured in global settings listed in above.	
Global Information	
Active Information	Switch# show spanning-tree active Spanning-Tree : Enabled Protocol : MSTP Root Address : 0012.77ee.eeee Priority : 32768 Root Path Cost : 0 Root Port : N/A Root Times : max-age 20, hello-time 2, forward-delay 15 Bridge Address : 0012.77ee.eeee Priority : 32768 Bridge Times : max-age 20, hello-time 2, forward-delay 15 BPDU transmission-limit : 3 Port Role State Cost Prio.Nbr Type Aggregated ------ ---------- ---------- -------- ---------- ------------ ------------ fa1 Designated Forwarding 200000 128.1 P2P(RSTP) N/A

	fa2 Designated Forwarding 200000 128.2 P2P(RSTP) N/A
RSTP Summary	Switch# show spanning-tree summary Switch is in rapid-stp mode. BPDU skewing detection disabled for the bridge. Backbonefast disabled for bridge. Summary of connected spanning tree ports : #Port-State Summary Blocking Listening Learning Forwarding Disabled -------- --------- -------- ---------- -------- 0 0 0 2 26 #Port Link-Type Summary AutoDetected PointToPoint SharedLink EdgePort ------------ ------------ ---------- -------- 9 0 1 9
Port Info	Switch# show spanning-tree port detail fa7 (Interface_ID) Rapid Spanning-Tree feature Enabled Port 128.6 as Disabled Role is in Disabled State Port Path Cost 200000, Port Identifier 128.6 RSTP Port Admin Link-Type is Auto, Oper Link-Type is Point-to-Point RSTP Port Admin Edge-Port is Enabled, Oper Edge-Port is Edge Designated root has priority 32768, address 0007.7c00.0112 Designated bridge has priority 32768, address 0007.7c60.1aec Designated Port ID is 128.6, Root Path Cost is 600000 Timers : message-age 0 sec, forward-delay 0 sec Link Aggregation Group: N/A, Type: N/A, Aggregated with: N/A BPDU: sent 43759 , received 4854 TCN : sent 0 , received 0 Forwarding-State Transmit count 12 Message-Age Expired count

MSTP Information–	
MSTP Configuration–	Switch# show spanning-tree mst configuration Current MST configuration (MSTP is Running) Name orenixnix] Revision 65535 Instance Vlans Mapped -------- ------------------------------------- 0 1,4-4094 1 2 2 -- Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D ---
Display all MST Information	Switch# show spanning-tree mst ###### MST00 vlans mapped: 1,4-4094 Bridge address 0012.77ee.eeee priority 32768 (sysid 0) Root this switch for CST and IST Configured max-age 2, hello-time 15, forward-delay 20, max-hops 20 Port Role State Cost Prio.Nbr Type ------ ---------- ---------- -------- ---------- ------------------ fa1 Designated Forwarding 200000 128.1 P2P Internal(MSTP) fa2 Designated Forwarding 200000 128.2 P2P Internal(MSTP) ###### MST01 vlans mapped: 2 Bridge address 0012.77ee.eeee priority 32768 (sysid 1) Root this switch for MST01 Port Role State Cost Prio.Nbr Type ------ ---------- ---------- -------- ---------- ------------------ fa1 Designated Forwarding 200000 128.1 P2P

	Internal(MSTP) fa2 Designated Forwarding 200000 128.2 P2P Internal(MSTP)
MSTP Root Information	Switch# show spanning-tree mst root MST Root Root Root Root Max Hello Fwd Instance Address Priority Cost Port age dly -------- -------------- -------- ----------- ------ ----- ----- ----- MST00 0012.77ee.eeee 32768 0 N/A 20 2 15 MST01 0012.77ee.eeee 32768 0 N/A 20 2 15 MST02 0012.77ee.eeee 32768 0 N/A 20 2 15
MSTP Instance Information	Switch# show spanning-tree mst 1 ###### MST01 vlans mapped: 2 Bridge address 0012.77ee.eeee priority 32768 (sysid 1) Root this switch for MST01 Port Role State Cost Prio.Nbr Type ------ ---------- ---------- -------- ---------- ------------------ fa1 Designated Forwarding 200000 128.1 P2P Internal(MSTP) fa2 Designated Forwarding 200000 128.2 P2P Internal(MSTP)
MSTP Port Information	Switch# show spanning-tree mst interface fa1 Interface fastethernet1 of MST00 is Designated Forwarding Edge Port : Edge (Edge) BPDU Filter : Disabled Link Type : Auto (Point-to-point) BPDU Guard : Disabled Boundary : Internal(MSTP) BPDUs : sent 6352, received 0 Instance Role State Cost Prio.Nbr Vlans mapped -------- ---------- ---------- -------- ---------- ---------------------

	0 Designated Forwarding 200000 128.1 1,4-4094 1 Designated Forwarding 200000 128.1 2 2 Designated Forwarding 200000 128.1 3
Multiple Super Ring	
Create or configure a Ring	Switch(config)# multiple-super-ring 1 Ring 1 created Switch(config-multiple-super-ring)# ***Note: 1 is the target Ring ID which is going to be created or configured.***
Super Ring Version	Switch(config-multiple-super-ring)# version default set default to rapid super ring rapid-super-ring rapid super ring super-ring super ring Switch(config-multiple-super-ring)# version rapid-super-ring
Priority	Switch(config-multiple-super-ring)# priority <0-255> valid range is 0 to 255 default set default Switch(config)# super-ring priority 100
Ring Port	Switch(config-multiple-super-ring)# port IFLIST Interface list, ex: fa1,fa3-5,gi8-10 cost path cost Switch(config-multiple-super-ring)# port fa1,fa2
Ring Port Cost	Switch(config-multiple-super-ring)# port cost <0-255> valid range is 0 or 255 default set default (128)valid range is 0 or 255 Switch(config-multiple-super-ring)# port cost 100 <0-255> valid range is 0 or 255 default set default (128)valid range is 0 or 255 Switch(config-super-ring-plus)# port cost 100 200 Set path cost success.
Rapid Dual Homing	Switch(config-multiple-super-ring)# rapid-dual-homing enable Switch(config-multiple-super-ring)# rapid-dual-homing disable

	Switch(config-multiple-super-ring)# rapid-dual-homing port IFLIST Interface name, ex: fastethernet1 or gi8 auto-detect up link auto detection IFNAME Interface name, ex: fastethernet1 or gi8 Switch(config-multiple-super-ring)# rapid-dual-homing port fa3,fa5-6 set Rapid Dual Homing port success. Note: auto-detect is recommended for dual Homing..
Ring Info	
Ring Info	Switch# show multiple-super-ring [Ring ID] [Ring1] Ring1 Current Status : Disabled Role : Disabled Ring Status : Abnormal Ring Manager : 0000.0000.0000 Blocking Port : N/A Giga Copper : N/A Configuration : Version : Rapid Super Ring Priority : 128 Ring Port : fa1, fa2 Path Cost : 100, 200 Dual-Homing II : Disabled Statistics : Watchdog sent 0, received 0, missed 0 Link Up sent 0, received 0 Link Down sent 0, received 0 Role Transition count 0 Ring State Transition count 1 Ring ID is optional. If the ring ID is typed, this command will only display the information of the target Ring.

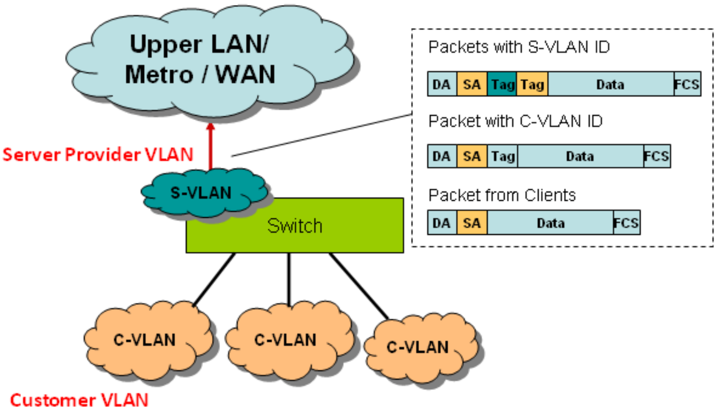
4.5 VLAN

A Virtual LAN (VLAN) is a "logical" grouping of nodes for the purpose of limiting a broadcast domain to specific members of a group without physically grouping the members together. That means, VLAN allows you to isolate network traffic so that only members of VLAN could receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is the logical equivalent of physically reconnecting a group of network devices to another Layer 2 switch, without actually disconnecting these devices from their original switches.

The switch supports 802.1Q VLAN. 802.1Q VLAN is also known as Tag-Based VLAN. This Tag-Based VLAN allows VLAN to be created across different switches. IEEE 802.1Q tag-based VLAN makes use of VLAN control information stored in a VLAN header attached to IEEE 802.3 packet frames. This tag contains a VLAN Identifier (VID) that indicates which VLAN a frame belongs to. Since each switch only has to check a frame's tag, without the need to dissect the contents of the frame, which saves a lot of computing resources within the switch.

QinQ

The QinQ is originally designed to expand the number of VLANs by adding a tag to the 802.1Q packets. The original VLAN is usually identified as Customer VLAN (C-VLAN) and the new added t–g - as Service VLAN(S-VLAN).



By adding the additional tag, QinQ increases the possible number of VLANs. After QinQ enabled, the switch can reach up to 256x256 VLANs. With different standard tags, it also improves the network security.

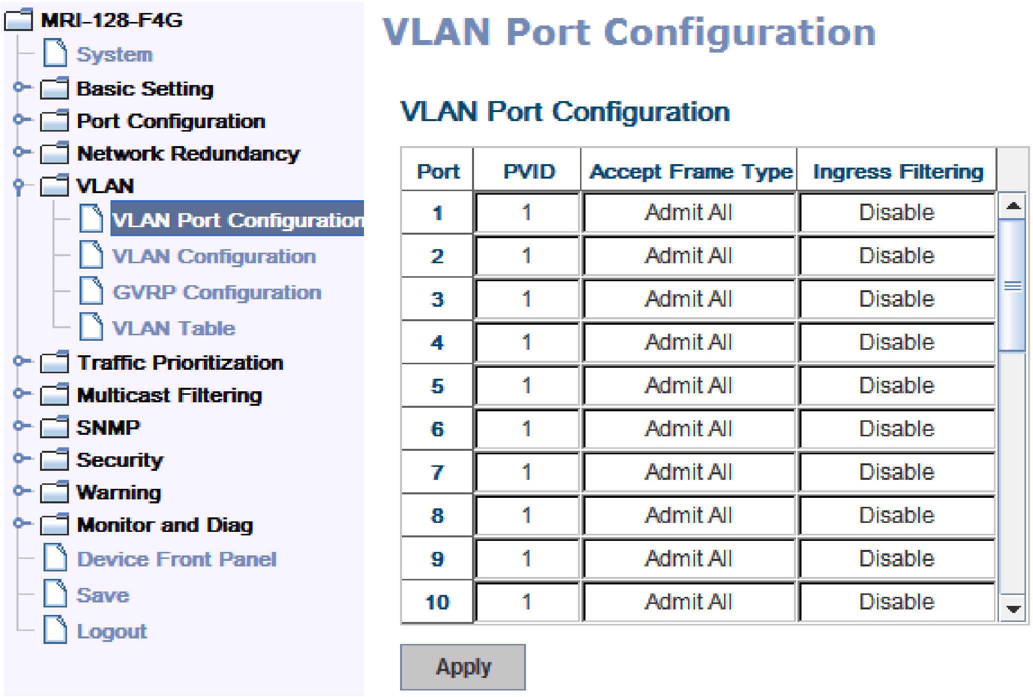
VLAN Configuration group enables you to Add/Remove VLAN, configure QinQ, port Ingress/Egress parameters and view VLAN table.

VLAN Configuration group enables you to Add/Remove VLAN, configure port Ingress/Egress parameters and view VLAN table.

Following commands are included in this section:

4.5.1 VLAN Port Configuration

VLAN Port Configuration allows you to set up VLAN port parameters to specific port. These parameters include PVID, Accept Frame Type and Ingress Filtering.



VLAN Port Configuration

VLAN Port Configuration

Port	PVID	Accept Frame Type	Ingress Filtering
1	1	Admit All	Disable
2	1	Admit All	Disable
3	1	Admit All	Disable
4	1	Admit All	Disable
5	1	Admit All	Disable
6	1	Admit All	Disable
7	1	Admit All	Disable
8	1	Admit All	Disable
9	1	Admit All	Disable
10	1	Admit All	Disable

PVID: The abbreviation of the **Port VLAN ID**. Enter port the VLAN ID. PVID allows the switches to identify which port belongs to which VLAN. To keep things simple, it is recommended that PVID is equivalent to VLAN IDs.

The values of PVIDs are from 0 to 4095. But, 0 and 4095 are reserved. You can’t input these two PVIDs and 1 is the default value and 2 to 4094 are valid and available.

Tunnel Mode: This is the new command for QinQ. The command includes None, 802.1Q Tunnel and 802.1Q Tunnel Uplink.

Following is the modes you can select.

None: Remain VLAN setting, no QinQ.

802.1Q Tunnel: The QinQ command applied to the ports which connect to the C-VLAN. The port receives tagged frame from the C-VLAN. Add a new tag (Port

VID) as S-VLAN VID. When the packets are forwarded to C-VLAN, the S-VLAN tag is removed.

After 802.1Q Tunnel mode is assigned to a port, the egress setting of the port should be "**Untag**", it indicates the egress packet is always untagged. This is configured in Static VLAN Configuration table. Please refer to the VLAN Configuration chapter in below.

802.1Q Tunnel Uplink: The QinQ command applied to the ports which connect to the S-VLAN. The port receives tagged frame from the S-VLAN. When the packets are forwarded to S-VLAN, the S-VLAN tag is kept.

After 802.1Q Tunnel Uplink mode is assigned to a port, the egress setting of the port should be "**Tag**", it indicates the egress packet is always tagged. This is configured in Static VLAN Configuration table. Please refer to the VLAN Configuration chapter in below.

For example, the VID of S-VLAN/Tunnel Uplink is 10, the VID of C-VLAN/Tunnel is 5. The 802.1Q Tunnel port receives tag 5 from C-VLAN, add tag 10 to the packet. When the packets are forwarded to S-VLAN, tag 10 is kept.

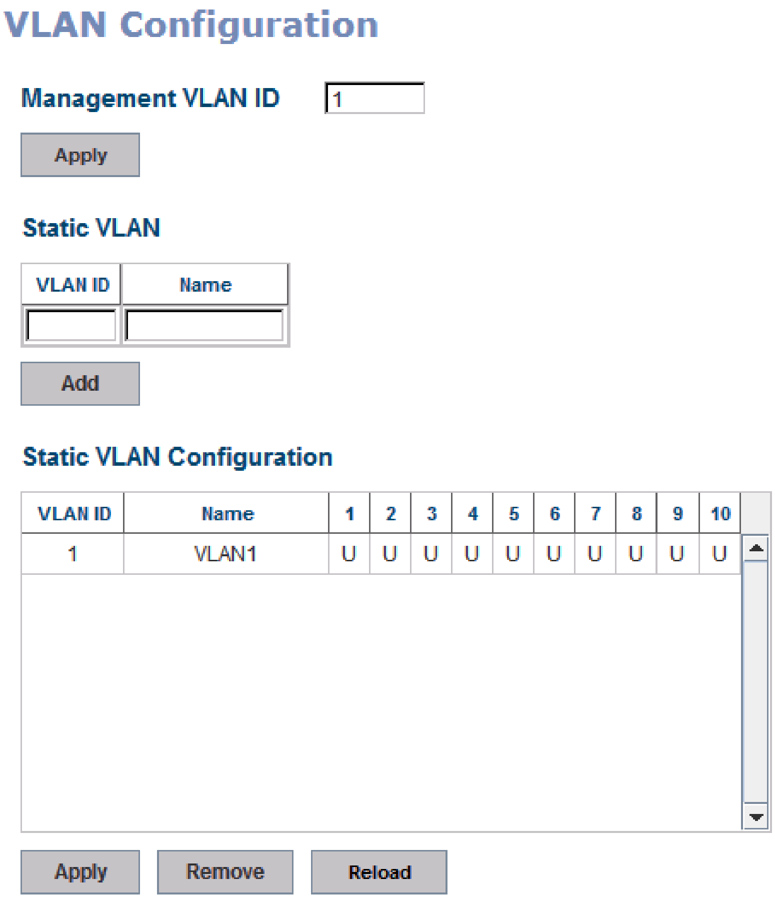
EtherType: This column allows you to define the EtherType manually. This is advanced QinQ parameter which allows defining the transmission packet type.

Accept Frame Type: This column defines the accepted frame type of the port. There are 2 modes you can select, **Admit All** and **Tag Only**. Admit All mode means that the port can accept both tagged and untagged packets. Tag Only mode means that the port can only accept tagged packets.

Ingress Filtering: Ingress filtering helps VLAN engine to filter out undesired traffic on a port. When Ingress Filtering is enabled, the port checks whether the incoming frames belong to the VLAN they claimed or not. Then the port determines if the frames can be processed or not. For example, if a tagged frame from Engineer VLAN is received, and Ingress Filtering is enabled, the switch will determine if the port is on the Engineer VLAN's Egress list. If it is, the frame can be processed. If it's not, the frame would be dropped.

4.5.2 VLAN Configuration

In this page, you can assign Management VLAN, create the static VLAN, and assign the Egress rule for the member ports of the VLAN.



VLAN Configuration

Management VLAN ID: 1

Static VLAN

VLAN ID	Name

Static VLAN Configuration

VLAN ID	Name	1	2	3	4	5	6	7	8	9	10
1	VLAN1	U	U	U	U	U	U	U	U	U	U

Management VLAN ID: The switch supports management VLAN. The management VLAN ID is the VLAN ID of the CPU interface so that **only member ports of the management VLAN can access the switch.** The default management VLAN ID is **1**.

Static VLAN: You can assign a VLAN ID and VLAN Name for new VLAN here.

VLAN ID is used by the switch to identify different VLANs. Valid VLAN ID is between 1 and 4094 and VLAN 1 is the default VLAN.

VLAN Name is a reference for network administrator to identify different VLANs. The available character is 12 for you to input. If you don't input VLAN name, the system will automatically assign VLAN name for the VLAN. The rule is VLAN (VLAN ID).

The steps to create a new VLAN: Type VLAN ID and NAME, and press **Add** to create a new VLAN. Then you can see the new VLAN in the Static VLAN Configuration table.

After created the VLAN, the status of the VLAN will remain in Unused until you add ports to the VLAN.

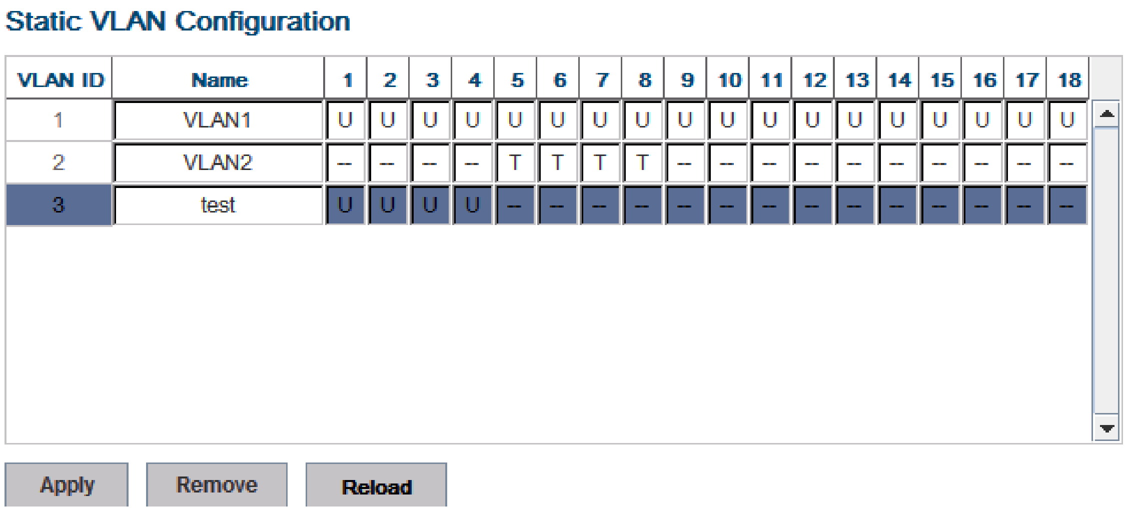
Note: *Before you change the management VLAN ID by Web and Telnet, remember that the port attached by the administrator should be the member* *port of the management VLAN; otherwise the administrator can’t access the switch via the network.*

***Note:** Currently the switch supports max 256 group VLAN.*

Static VLAN Configuration

You can see the created VLANs and specify the egress (outgoing) port rule to be **Untagged or Tagged**.

Static VLAN Configuration table. You can see that new VLAN 3 is created. VLAN name is test. Egress rules of the ports are not configured now.



Static VLAN Configuration

VLAN ID	Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	VLAN1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U
2	VLAN2	--	--	--	--	T	T	T	T	--	--	--	--	--	--	--	--	--	--
3	test	U	U	U	U	--	--	--	--	--	--	--	--	--	--	--	--	--	--

-- : Not available

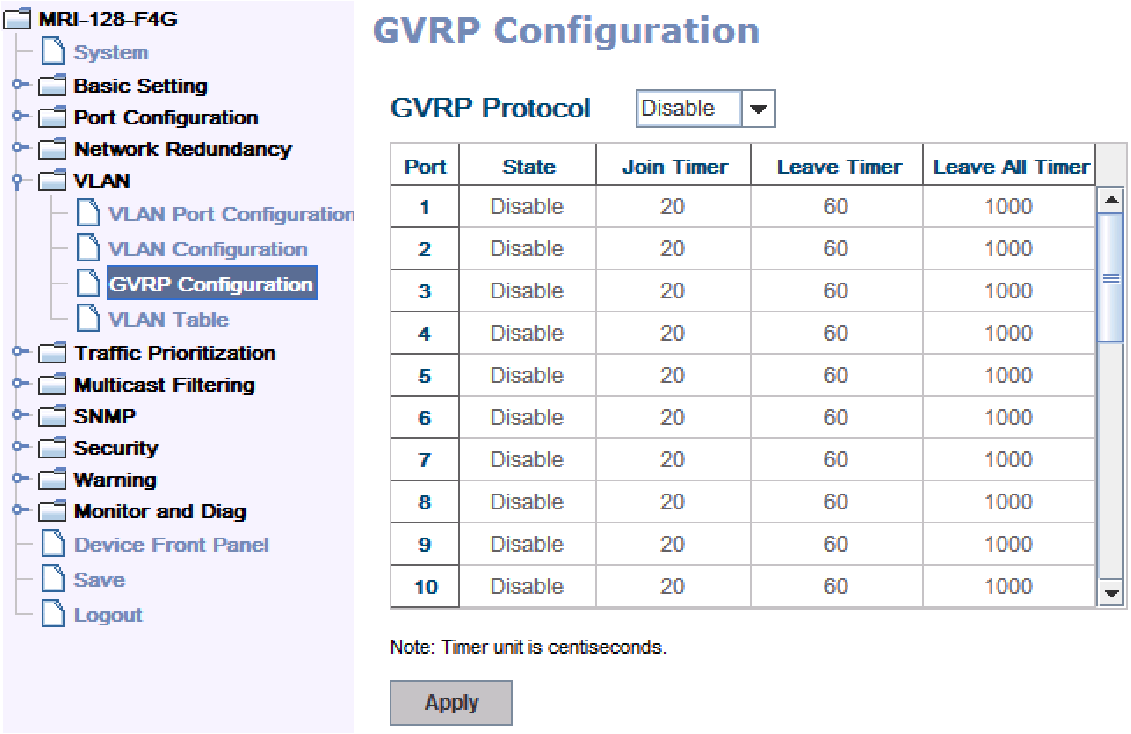
U: **Untag**: Indicates that egress/outgoing frames are not VLAN tagged.

T : **Tag**: Indicates that egress/outgoing frames are to be VLAN tagged.

Steps to configure Egress rules: Select the VLAN ID. Entry of the selected VLAN turns to light blue. Assign Egress rule of the ports to **U** or **T**. Press **Apply** to apply the setting. If you want to remove one VLAN, select the VLAN entry. Then press **Remove** button.

4.5.3 GVRP configuration

GVRP allows users to set-up VLANs automatically rather than manual configuration on every port of every switch in the network. In low volume and stable network, the GVRP can reduce the configuration effort. For high volume and high secure request network, the Static VLAN configuration is always preferred.



GVRP Configuration

GVRP Protocol: Disable

Port	State	Join Timer	Leave Timer	Leave All Timer
1	Disable	20	60	1000
2	Disable	20	60	1000
3	Disable	20	60	1000
4	Disable	20	60	1000
5	Disable	20	60	1000
6	Disable	20	60	1000
7	Disable	20	60	1000
8	Disable	20	60	1000
9	Disable	20	60	1000
10	Disable	20	60	1000

Note: Timer unit is centiseconds.

GVRP Protocol: Allow user to enable/disable GVRP globally.

State: After enable GVRP globally, here still can enable/disable GVRP by port.

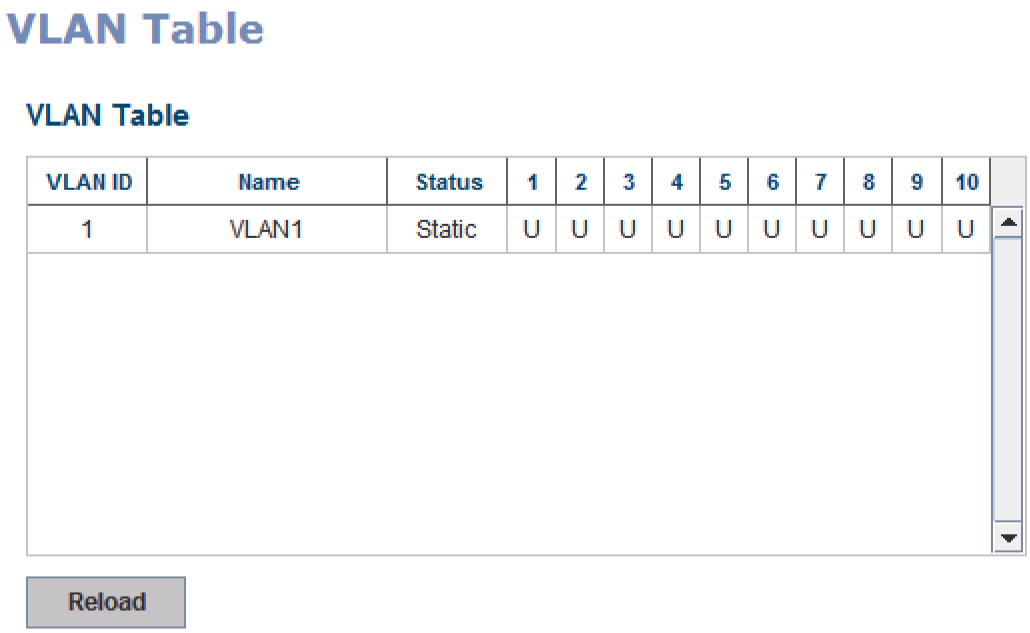
Join Timer: Controls the interval of sending the GVRP Join BPDU. An instance of this timer is required on a per-Port, per-GARP Participant basis.

Leave Timer: Control the time to release the GVRP reservation after received the GVRP Leave BPDU. An instance of the timer is required for each state machine that is in the LV state.

Leave All Timer: Controls the period to initiate the garbage collection of registered VLAN. The timer is required on a per-Port, per-GARP Participant basis.

4.5.4 VLAN Table

This table shows you current settings of your VLAN table, including VLAN ID, Name, Status, and Egress rule of the ports.



VLAN ID	Name	Status	1	2	3	4	5	6	7	8	9	10
1	VLAN1	Static	U	U	U	U	U	U	U	U	U	U

VLAN ID: ID of the VLAN.

Name: Name of the VLAN.

Status: Static shows this is a manually configured static VLAN. **Unused** means this VLAN is created by UI/CLI and has no member ports. This VLAN is not workable yet. **Dynamic** means this VLAN is learnt by GVRP.

After created the VLAN, the status of this VLAN will remain in Unused status until you add ports to the VLAN.

4.5.5 CLI Commands of the VLAN

Command Lines of the VLAN port configuration, VLAN configuration and VLAN table display

Feature	Command Line
VLAN Port Configuration	
Port Interface Configuration	Switch# conf ter Switch(config)# interface fa5 Switch(config-if)#
VLAN Port PVID	Switch(config-if)# switchport trunk native vlan 2 Set port default vlan id to 2 success
QinQ Tunnel Mode	Switch(config-if)# switchport dot1q-tunnel mode Set the interface as an IEEE 802.1Q tunnel mode Switch(config-if)# switchport dot1q-tunnel mode

802.1Q Tunnel = access 802.1Q Tunnel Uplink = uplink	access Set the interface as an access port of IEEE 802.1Q tunnel mode uplink Set the interface as an uplink port of IEEE 802.1Q tunnel mode
Port Accept Frame Type	Switch(config)# inter fa1 Switch(config-if)# acceptable frame type all any kind of frame type is accepted! Switch(config-if)# acceptable frame type vlantaggedonly only vlan-tag frame is accepted!
Ingress Filtering (for fast Ethernet port 1)	Switch(config)# interface fa1 Switch(config-if)# ingress filtering enable ingress filtering enable Switch(config-if)# ingress filtering disable ingress filtering disable
Egress rule – Untagged (for VLAN 2)	Switch(config-if)# switchport access vlan 2 switchport access vlan - success
Egress rule – Tagged (for VLAN 2)	Switch(config-if)# switchport trunk allowed vlan add 2
Display – Port Ingress Rule (PVID, Ingress Filtering, Acceptable Frame Type)	Switch# show interface fa1 Interface fastethernet1 Administrative Status : Enable Operating Status : Not Connected Duplex : Auto Speed : Auto Flow Control :off Default Port VLAN ID: 2 Ingress Filtering : Disabled Acceptable Frame Type : All Port Security : Disabled Auto Negotiation : Enable Loopback Mode : None STP Status: disabled Default CoS Value for untagged packets is 0. Mdix mode is Auto. Medium mode is Copper.

Display – Port Egress Rule (Egress rule, IP address, status)	Switch# show running-config …… ! interface fastethernet1 switchport access vlan 1 switchport access vlan 3 switchport trunk native vlan 2 ……. interface vlan1 ip address 192.168.2.8/24 no shutdown
QinQ Information – 802.1Q Tunnel	Switch# show dot1q-tunnel dot1q-tunnel mode por 1 : normal por 2 : normal por 3 : normal por 4 : normal por 5 : access por 6 : uplink por 7 : normal por 8 : normal por 9 : normal port 10 : normal–
QinQ Information – Show Running	Switch# show running-config Building configuration... Current configuration: hostname Switch vlan learning independent ……… ……… interface fastethernet5 switchport access vlan add 1-2,10 switchport dot1q-tunnel mode access ! interface fastethernet6

	switchport access vlan add 1-2 switchport trunk allowed vlan add 10 switchport dot1q-tunnel mode uplink !
VLAN Configuration	
Create VLAN (2)	Switch(config)# vlan 2 vlan 2 success Switch(config)# interface vlan 2 Switch(config-if)# *Note: In CLI configuration, you should create a VLAN interface first. Then you can start to add/remove ports. Default status of the created VLAN is unused until you add member ports to it.*
Remove VLAN	Switch(config)# no vlan 2 no vlan success *Note: You can only remove the VLAN when the VLAN is in unused mode.*
VLAN Name	Switch(config)# vlan 2 vlan 2 has exists Switch(config-vlan)# name v2 Switch(config-vlan)# no name *Note: Use no name to change the name to default name, VLAN VID.*
VLAN description	Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# description this is the VLAN 2 Switch(config-if)# no description ->Delete the description.
IP address of the VLAN	Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# ip address 192.168.2.200/24

	Switch(config-if)# no ip address 192.168.2.200/24 ->Delete the IP address
Create multiple VLANs (VLAN 5-10)	Switch(config)# interface vlan 5-10
Shut down VLAN	Switch(config)# interface vlan 2 Switch(config-if)# shutdown Switch(config-if)# no shutdown ->Turn on the VLAN
Display – VLAN table	Switch# sh vlan VLAN Name Status Trunk Ports Access Ports ---- ------------ ------- -------------------------- -------------------------- 1 VLAN1 Static - fa1-7,gi8-10 2 VLAN2 Unused - - 3 test Static fa4-7,gi8-10 fa1-3,fa7,gi8-10

Display – VLAN interface information	Switch# show interface vlan1
	interface vlan1 is up, line protocol detection is disabled
	    index 14 metric 1 mtu 1500
	<UP,BROADCAST,RUNNING,MULTICAST>
	    HWaddr: 00:07:7c:ff:01:b0
	    inet 192.168.2.200/24 broadcast 192.168.2.255
	        input packets 639, bytes 38248, dropped 0, multicast packets 0
	        input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
	        output packets 959, bytes 829280, dropped 0
	        output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
	        collisions 0

GVRP configuration	
GVRP enable/disable	Switch(config)# gvrp mode disable Disable GVRP feature globally on the switch

	enable Enable GVRP feature globally on the switch Switch(config)# gvrp mode enable Gvrp is enabled on the switch!
Configure GVRP timer Join timer /Leave timer/ LeaveAll timer	Switch(config)# inter fa1 Switch(config-if)# garp timer <10-10000> Switch(config-if)# garp timer 20 60 1000 Note: The unit of these timer is centisecond
Management VLAN	
Management VLAN	Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# no shutdown
Display	Switch# show running-config .... ! interface vlan1 ip address 192.168.2.200/24 ip igmp no shutdown ! ....

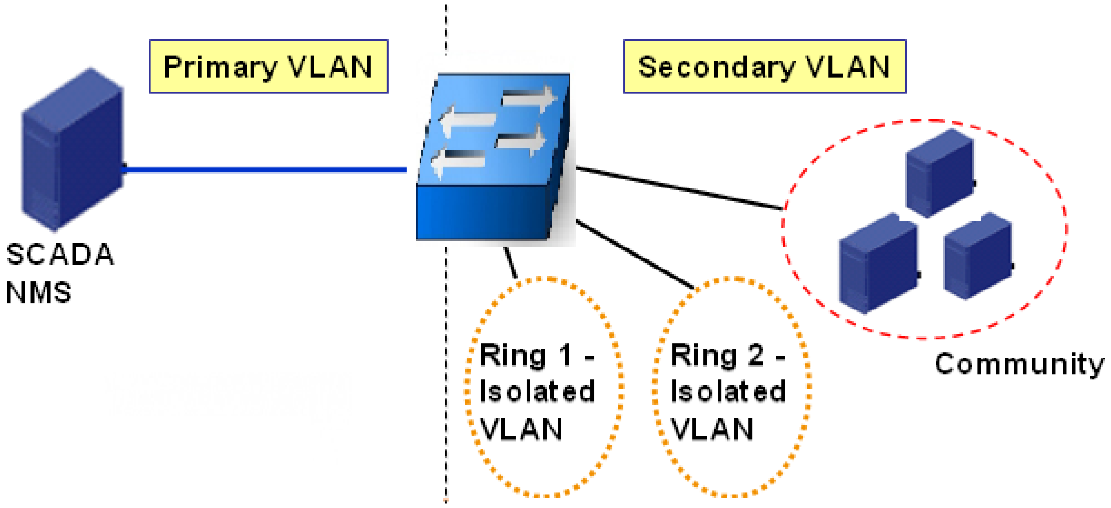
4.6 Private VLAN

The private VLAN helps to resolve the primary VLAN ID shortage, client ports' isolation and network security issues. The Private VLAN provides primary and secondary VLAN within a single switch.

Primary VLAN: The uplink port is usually the primary VLAN. A primary VLAN contains promiscuous ports that can communicate with lower Secondary VLANs.

Secondary VLAN: The client ports are usually defined within secondary VLAN. The secondary VLAN includes Isolated VLAN and Community VLAN. The client ports can be isolated VLANs or can be grouped in the same Community VLAN. The ports within the same community VLAN can communicate with each other. However, the isolated VLAN ports can Not.

The figure shows the typical Private VLAN network. The SCADA/Public Server or NMS workstation is usually located in primary VLAN. The clients PCs or Rings are located within Secondary.



Private VLAN (PVLAN) Configuration group enables you to Configure PVLAN, PVLAN Port and see the PVLAN Information.

Following commands are included in this group:

4.6.1 PVLAN Configuration

4.6.2 PVLAN Port Configuration

4.6.3 Private VLAN Information

4.6.4 CLI Commands of the PVLAN

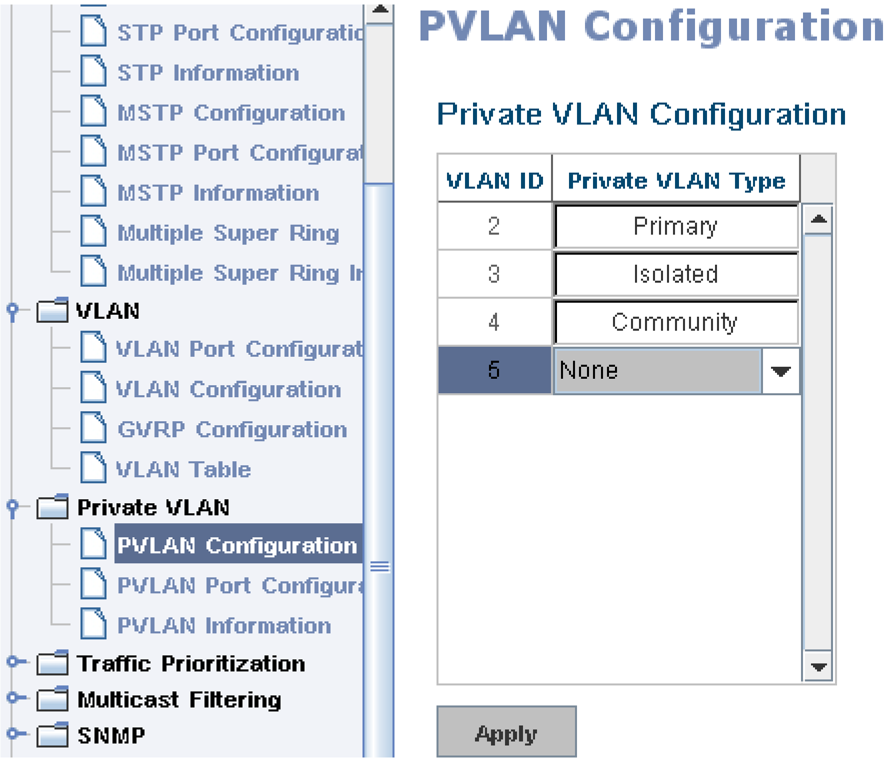
4.6.1 PVLAN Configuration

PVLAN Configuration allows you to assign Private VLAN type. After created VLAN in VLAN Configuration page, the available VLAN ID will display here. Choose the Private VLAN types for each VLAN you want configure.

None: The VLAN is Not included in Private VLAN.

Primary: The VLAN is the Primary VLAN. The member ports can communicate with secondary ports.

Isolated: The VLAN is the Isolated VLAN. The member ports of the VLAN are isolated.



PVLAN Configuration

Private VLAN Configuration

VLAN ID	Private VLAN Type
2	Primary
3	Isolated
4	Community
5	None

Community: The VLAN is the Community VLAN. The member ports of the VLAN can communicate with each other.

4.6.2 PVLAN Port Configuration

PVLAN Port Configuration page allows configure Port Configuration and Private VLAN Association.

Private VLAN Association

Secondary VLAN: After the Isolated and Community VLAN Type is assigned in Private VLAN Configuration page, the VLANs are belonged to the Secondary VLAN and displayed here.

Primary VLAN: After the Primary VLAN Type is assigned in Private VLAN Configuration page, the secondary VLAN can associate to the Primary VLAN ID. Select the Primary VLAN ID here.

Note: Before configuring PVLAN port type, the Private VLAN Association should be done first.

Port Configuraion

PVLAN Port T pe :

Normal: The Normal port is None PVLAN ports; it remains its original VLAN setting.

Host: The Host type ports can be mapped to the Secondary VLAN.

Promiscuous: The promiscuous port can be associated to the Primary VLAN.

VLAN ID: After assigned the port type, the web UI display the available VLAN ID the port can associate to.

For example:

1. VLAN Create: VLAN 2-5 are created in VLAN Configuration page.

2. Private VLAN Type: VLAN 2-5 has its Private VLAN Type configured in Private VLAN Configuration page.

VLAN 2 is belonged to Primary VLAN.

VLAN 3-5 are belonged to secondary VLAN (Isolated or Community).

3. Private VLAN Association: Associate VLAN 3-5 to VLAN 2 in Private VLAN Association first.

4. Private VLAN Port Configuration

VLAN 2 – Primary -> The member port of VLAN 2 is promiscuous port.

VLAN 3 – Isolated -> The Host port can be mapped to VLAN 3.

VLAN 4 – Community -> The Host port can be mapped to VLAN 3.

VLAN 5 – Community -> The Host port can be mapped to VLAN

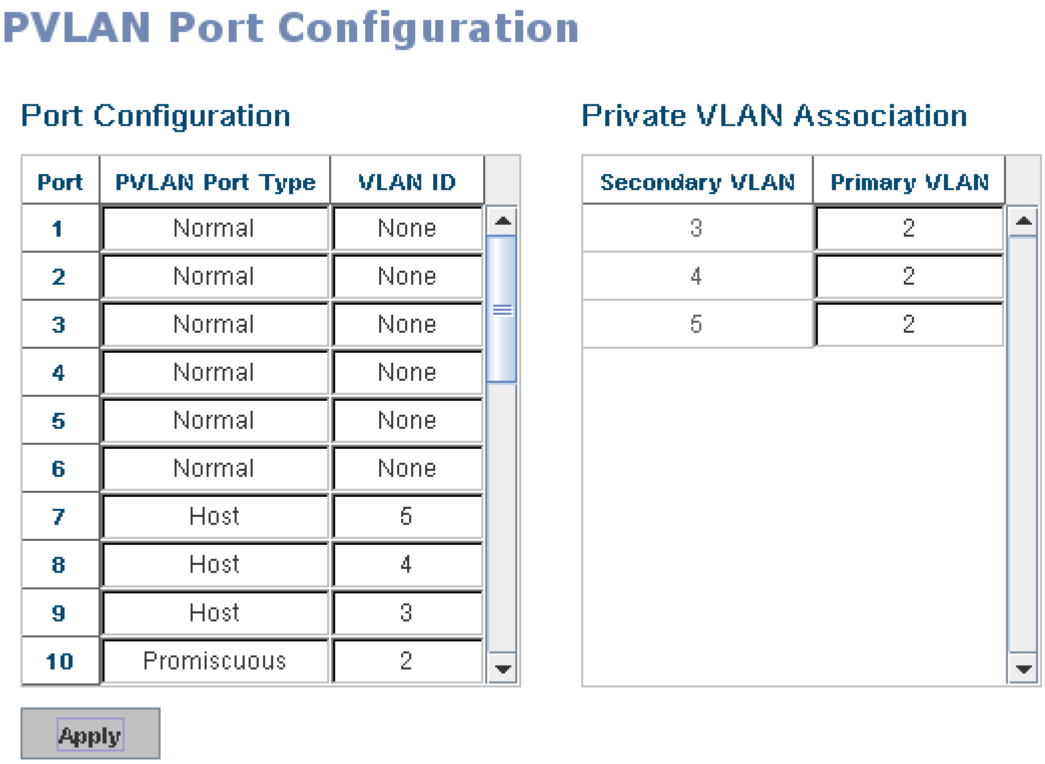
5. Result:

VLAN 2 -> VLAN 3, 4, 5; member ports can communicate with ports in secondary VLAN.

VLAN 3 -> VLAN 2, member ports are isolated, but it can communicate with member port of VLAN 2..

VLAN 4 -> VLAN 2, member ports within the community can communicate with each other and communicate with member port of VLAN 2.

VLAN 5 -> VLAN 2, member ports within the community can communicate with each other and communicate with member port of VLAN 2.



PVLAN Port Configuration

Port Configuration

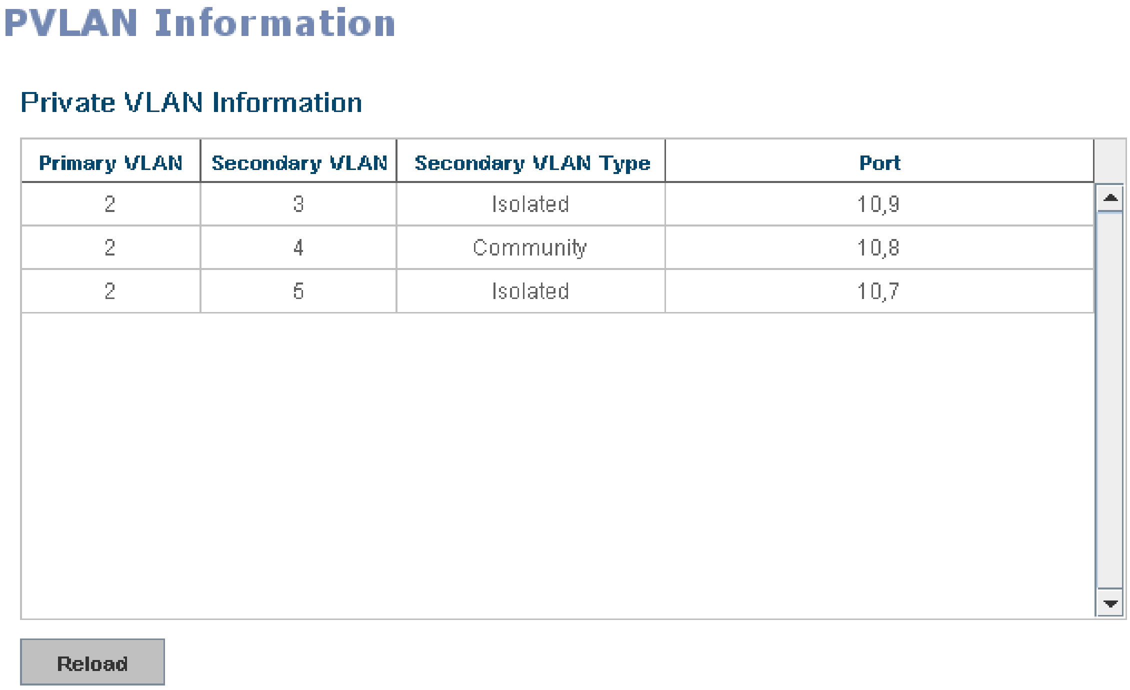
Port	PVLAN Port Type	VLAN ID
1	Normal	None
2	Normal	None
3	Normal	None
4	Normal	None
5	Normal	None
6	Normal	None
7	Host	5
8	Host	4
9	Host	3
10	Promiscuous	2

Private VLAN Association

Secondary VLAN	Primary VLAN
3	2
4	2
5	2

4.6.3 Private VLAN Information

This page allows you to see the Private VLAN information.



PVLAN Information

Private VLAN Information

Primary VLAN	Secondary VLAN	Secondary VLAN Type	Port
2	3	Isolated	10,9
2	4	Community	10,8
2	5	Isolated	10,7

4.6.4 CLI Command of the PVLAN

Command Lines of the Private VLAN configuration

Feature	Command Line
Private VLAN Configuration	
Create VLAN	Switch(config)# vlan 2 vlan 2 success Switch(config-vlan)# end End current mode and change to enable mode exit Exit current mode and down to previous mode list Print command list name Assign a name to vlan no no private-vlan Configure a private VLAN
Private VLAN Type Choose the Types Primary Type Isolated Type Community Type	**Go to the VLAN you want configure first.** Switch(config)# vlan (VID) Switch(config-vlan)# private-vlan community Configure the VLAN as an community private VLAN isolated Configure the VLAN as an isolated private VLAN primary Configure the VLAN as a primary private VLAN Switch(config-vlan)# private-vlan primary <cr> Switch(config-vlan)# private-vlan isolated <cr> Switch(config-vlan)# private-vlan community <cr>
Private VLAN Port Configuraiton	

Go to the port configuraiton	Switch(config)# interface (port_number, ex: gi9)
	Switch(config-if)# switchport private-vlan
	  host-association Set the private VLAN host association
	  mapping map primary VLAN to secondary VLAN

Private VLAN Port Type Promiscuous Port Type Host Port Type	Switch(config-if)# switchport mode private-vlan Set private-vlan mode Switch(config-if)# switchport mode private-vlan host Set the mode to private-vlan host promiscuous Set the mode to private-vlan promiscuous Switch(config-if)# switchport mode private-vlan promiscuous <cr> Switch(config-if)# switchport mode private-vlan host <cr>
Private VLAN Port Configuration	Switch(config)# interface gi9

PVLAN Port Type Host Association primary to secondary (The command is only available for host port.)	Switch(config-if)# switchport mode private-vlan host Switch(config-if)# switchport private-vlan host-association <2-4094> Primary range VLAN ID of the private VLAN port association Switch(config-if)# switchport private-vlan host-association 2 <2-4094> Secondary range VLAN ID of the private VLAN port association Switch(config-if)# switchport private-vlan host-association 2 3
Mapping primary to secondary VLANs (This command is only available for promiscuous port)	Switch(config)# interface gi10 Switch(config-if)# switchport mode private-vlan promiscuous Switch(config-if)# switchport private-vlan mapping 2 add 3 Switch(config-if)# switchport private-vlan mapping 2 add 4 Switch(config-if)# switchport private-vlan mapping 2 add 5
Private VLAN Information	
Private VLAN Information	Switch# show vlan private-vlan FLAGS: I -> Isolated P -> Promiscuous C -> Community Primary Secondary Type Ports ------- --------- ----------------- --------------------- 2 3 Isolated gi10(P),gi9(I) 2 4 Community gi10(P),gi8(C) 2 5 Community gi10(P),fa7(C),gi9(I) 10 - - -
PVLAN Type	Switch# show vlan private-vlan type Vlan Type Ports ---- ----------------- ----------------- 2 primary gi10 3 isolated gi9 4 community gi8 5 community fa7,gi9 10 primary -
Host List	Switch# show vlan private-vlan port-list Ports Mode Vlan ----- ----------- ---- 1 normal - 2 normal - 3 normal - 4 normal - 5 normal - 6 normal - 7 host 5 8 host 4 9 host 3

	10 promiscuous 2
Running Config Information	Switch# show run Building configuration... Current configuration: hostname Switch vlan learning independent ! vlan 1 !
Private VLAN Type	vlan 2 private-vlan primary ! vlan 3 private-vlan isolated ! vlan 4 private-vlan community ! vlan 5 private-vlan community ! ....
Private VLAN Port Information	interface fastethernet7 switchport access vlan add 2,5 switchport trunk native vlan 5 switchport mode private-vlan host switchport private-vlan host-association 2 5 ! interface gigabitethernet8 switchport access vlan add 2,4 switchport trunk native vlan 4 switchport mode private-vlan host switchport private-vlan host-association 2 4 ! interface gigabitethernet9 switchport access vlan add 2,5 switchport trunk native vlan 5 switchport mode private-vlan host switchport private-vlan host-association 2 3 ! interface gigabitethernet10 switchport access vlan add 2,5 switchport trunk native vlan 2 switchport mode private-vlan promiscuous switchport private-vlan mapping 2 add 3-5 ……… ……..

4.7 Traffic Prioritization

Quality of Service (QoS) provides traffic prioritization mechanism and can also help to alleviate congestion problems and ensure high-priority traffic is delivered first. This section allows you to configure Traffic Prioritization settings for each port with regard to setting priorities.

The switch QOS supports four physical queues, weighted fair queuing (WRR) and Strict Priority scheme, which follows 802.1p COS tag and IPv4 TOS/DiffServ information to prioritize the traffic of your industrial network.

Following commands are included in this chapter:

4.7.1 QoS Setting

4.7.2 Port-based Queue Mapping

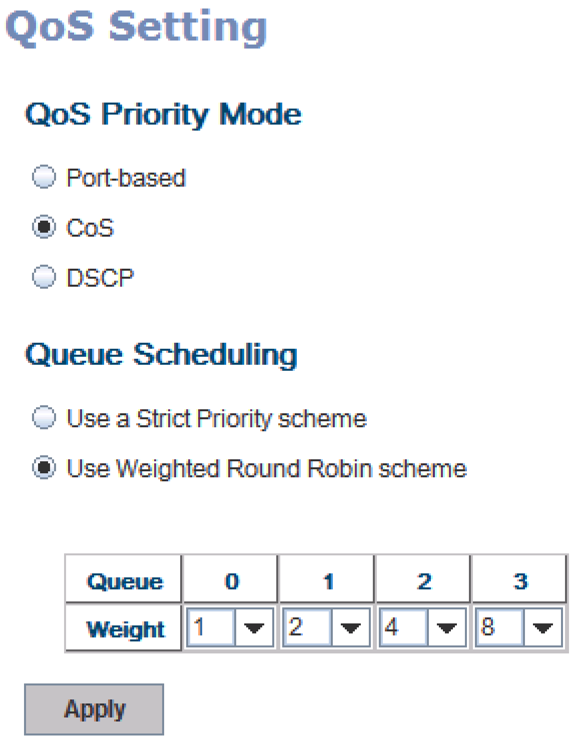
4.7.3 CoS-Queue Mapping

4.7.4 DSCP-Queue Mapping

4.7.5 CLI Commands of the Traffic Prioritization

4.7.1 QoS Setting

In QoS setting, you should choose the QoS Priority Mode first, Port-Based, Cos or DSCP modes. Choose the preferred mode and you can configure the next settings in its own configuration pages. The other page of the mode you don't select can't be configured.



QoS Setting

QoS Priority Mode

○ Port-based

● CoS

○ DSCP

Queue Scheduling

○ Use a Strict Priority scheme

● Use Weighted Round Robin scheme

Queue	0	1	2	3
Weight	1	2	4	8

Queue Scheduling

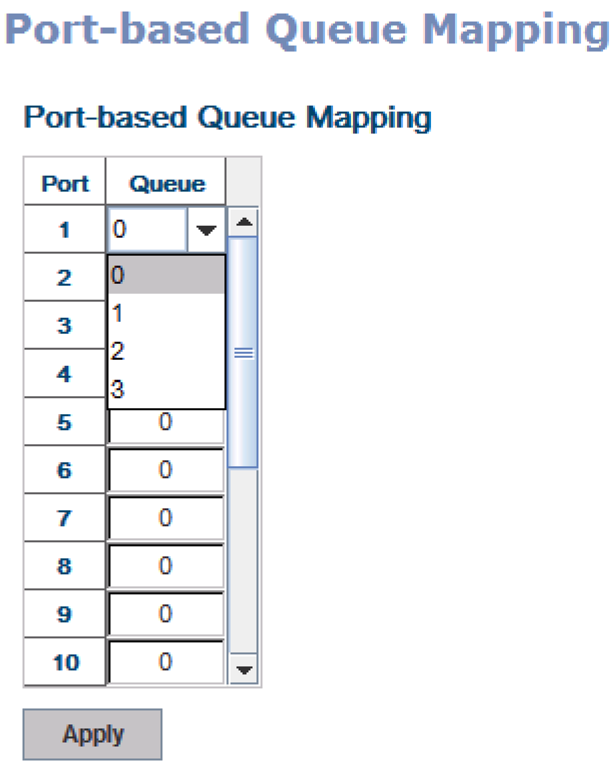
You can select the Queue Scheduling rule as follows:

Use a strict priority scheme. Packets with higher priority in the queue will always be processed first, except that there is no packet with higher priority.

Use Weighted Round Robin scheme. This scheme allows users to assign new weight ratio for each class. The 10 is the highest ratio. The ratio of each class is as below:

Wx / W0 + W1 + W2 + W3 (Total volume of Queue 0-3)

4.7.2 Port-based Queue Mapping



Port-based Queue Mapping

Port-based Queue Mapping

Port	Queue
1	0
2	
3	
4	
5	0
6	0
7	0
8	0
9	0
10	0

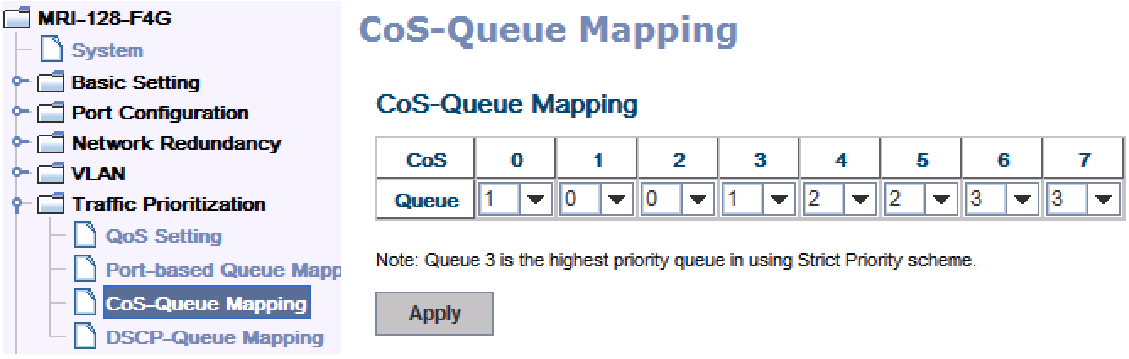
Choose the Queue value of each port, the port then has its default priority. The Queue 3 is the highest port-based queue, 0 is the lowest queue. The traffic injected to the port follows the queue level to be forwarded, but the outgoing traffic doesn’t bring the queue level to next switch.

After configuration, press **Apply** to enable the settings.

4.7.3 CoS-Queue Mapping

This page is to change CoS values to Physical Queue mapping table. Since the switch fabric of Switch only supports four physical queues, Lowest, Low, Middle and High. Users should therefore assign how to map CoS value to the level of the physical queue.

Users can freely assign the mapping table or follow the suggestion of the 802.1p standard. The switch uses 802.p suggestion as default values. You can find CoS values 1 and 2 are mapped to physical Queue 0, the lowest queue. CoS values 0 and 3 are mapped to physical Queue 1, the low/normal physical queue. CoS values 4 and 5 are mapped to physical Queue 2, the middle physical queue. CoS values 6 and 7 are mapped to physical Queue 3, the high physical queue.



CoS-Queue Mapping

CoS-Queue Mapping

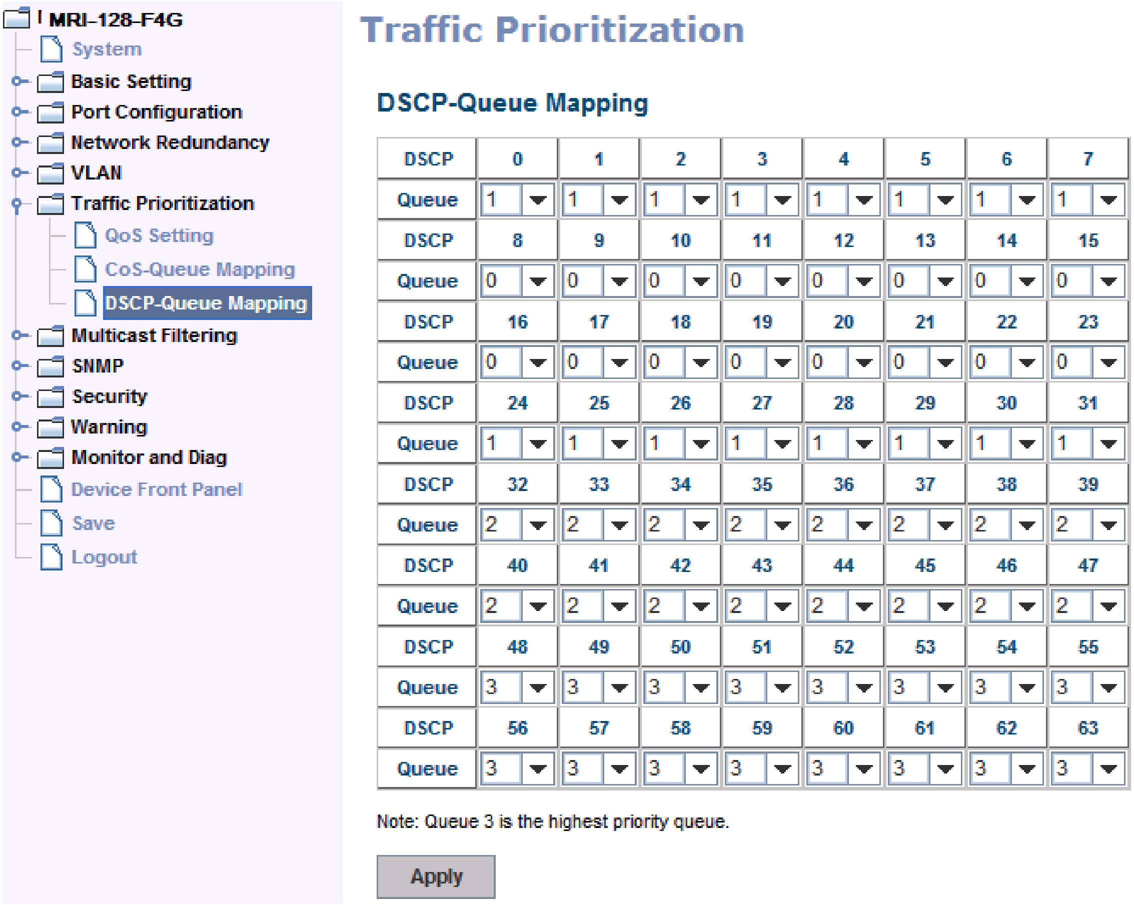
CoS	0	1	2	3	4	5	6	7
Queue	1	0	0	1	2	2	3	3

Note: Queue 3 is the highest priority queue in using Strict Priority scheme.

After configuration, press **Apply** to enable the settings.

4.7.4 DSCP-Queue Mapping

This page is to change DSCP values to Physical Queue mapping table. Since the switch fabric of Switch only supports four physical queues, Lowest, Low, Middle and High. Users should therefore assign how to map DSCP value to the level of the physical queue. Users can freely change the mapping table to follow the upper layer 3 switch or routers' DSCP setting.



Traffic Prioritization

DSCP-Queue Mapping

DSCP	0	1	2	3	4	5	6	7
Queue	1	1	1	1	1	1	1	1
DSCP	8	9	10	11	12	13	14	15
Queue	0	0	0	0	0	0	0	0
DSCP	16	17	18	19	20	21	22	23
Queue	0	0	0	0	0	0	0	0
DSCP	24	25	26	27	28	29	30	31
Queue	1	1	1	1	1	1	1	1
DSCP	32	33	34	35	36	37	38	39
Queue	2	2	2	2	2	2	2	2
DSCP	40	41	42	43	44	45	46	47
Queue	2	2	2	2	2	2	2	2
DSCP	48	49	50	51	52	53	54	55
Queue	3	3	3	3	3	3	3	3
DSCP	56	57	58	59	60	61	62	63
Queue	3	3	3	3	3	3	3	3

Note: Queue 3 is the highest priority queue.

After configuration, press **Apply** to enable the settings.

4.7.5 CLI Commands of the Traffic Prioritization

Command Lines of the Traffic Prioritization configuration

Feature	Command Line
QoS Setting	
Queue Scheduling – Strict Priority	Switch(config)# qos queue-sched sp Strict Priority wrr Weighted Round Robin Switch(config)# qos queue-sched sp The queue scheduling scheme is setting to Strict Priority.
Queue Scheduling - WRR	Switch(config)# qos queue-sched wrr <1-10> Weights for COS queue 0 (queue_id 0) Switch(config)# qos queue-sched wrr 10 <1-10> Weights for COS queue 1 (queue_id 1) .... Switch(config)# qos queue-sched wrr 1 2 3 4

	The queue scheduling scheme is setting to Weighted Round Robin. ***Assign the ratio for the 4 classes of service.***
Port Setting – CoS (Default Port Priority)	Switch(config)# interface **fa1** Switch(config-if)# qos priority <0-3> Assign a priority queue Switch(config-if)# qos priority 3 The priority queue is set 3 ok. ***Note: When change the port setting, you should Select the specific port first. Ex: fa1 means fast Ethernet port 1.***
QoS Priority Mode	Switch(config)# qos priority cos CoS dscp DSCP/TOS port-based Port-based Switch(config)# qos priority dscp Switch# show qos priority QoS Priority Mode: DSCP
Display - Queue Scheduling	Switch# show qos queue-sched QoS queue scheduling scheme : Weighted Round Robin COS queue 0 = 1 COS queue 1 = 2 COS queue 2 = 3 COS queue 3 = 4
Display – Port Priority Setting (Port Default Priority)	Switch# show qos port-priority Port Default Priority : Port Priority Queue -----+---- 1 7 2 0 3 0 4 0 5 0 ……….

	25 0
	26 0
	27 0
	28 0

CoS-Queue Mapping	
Format	Switch(config)# qos cos-map PRIORITY Assign an priority (7 highest) Switch(config)# qos cos-map 1 QUEUE Assign an queue (0-3) ***Note: Format: qos cos-map priority_value queue_value***
Map CoS 0 to Queue 1	Switch(config)# qos cos-map 0 1 The CoS to queue mapping is set ok.
Map CoS 1 to Queue 0	Switch(config)# qos cos-map 1 0 The CoS to queue mapping is set ok.
Map CoS 2 to Queue 0	Switch(config)# qos cos-map 2 0 The CoS to queue mapping is set ok.
Map CoS 3 to Queue 1	Switch(config)# qos cos-map 3 1 The CoS to queue mapping is set ok.
Map CoS 4 to Queue 2	Switch(config)# qos cos-map 4 2 The CoS to queue mapping is set ok.
Map CoS 5 to Queue 2	Switch(config)# qos cos-map 5 2 The CoS to queue mapping is set ok.
Map CoS 6 to Queue 3	Switch(config)# qos cos-map 6 3 The CoS to queue mapping is set ok.
Map CoS 7 to Queue 3	Switch(config)# qos cos-map 7 3 The CoS to queue mapping is set ok.
Display – CoS-Queue mapping	Switch# sh qos cos-map CoS to Queue Mapping : CoS Queue ---- + ------ 0 1 1 0 2 0 3 1 4 2 5 2

<table>
<tr><td></td><td>6 3
7 3</td></tr>
<tr><td colspan="2"><b>DSCP-Queue Mapping</b></td></tr>
<tr><td>Format</td><td>Switch(config)# qos dscp-map
  <0-63>   Assign an priority (63 highest)
Switch(config)# qos dscp-map 0
  <0-3>   Assign an queue (0-3)

<b><i>Format: qos dscp-map priority_value queue_value</i></b></td></tr>
<tr><td>Map DSCP 0 to Queue 1</td><td>Switch(config)# qos dscp-map 0 1
The TOS/DSCP to queue mapping is set ok.</td></tr>
<tr><td>Display – DSCO-Queue mapping</td><td>Switch# show qos dscp-map
DSCP to Queue Mapping : (dscp = d1 d2)

    d2| 0 1 2 3 4 5 6 7 8 9
d1 |
-----+----------------------
    0 | 1 1 1 1 1 1 1 1 0 0
    1 | 0 0 0 0 0 0 0 0 0 0
    2 | 0 0 0 0 1 1 1 1 1 1
    3 | 1 1 2 2 2 2 2 2 2 2
    4 | 2 2 2 2 2 2 2 2 3 3
    5 | 3 3 3 3 3 3 3 3 3 3
    6 | 3 3 3 3</td></tr>
</table>

4.8 Multicast Filtering

For multicast filtering, the switch uses IGMP Snooping technology. IGMP (Internet Group Management Protocol) is an Internet Protocol that provides a way for internet device to report its multicast group membership to adjacent routers. Multicasting allows one computer on the internet to send data to a multitude of other computers that have identified themselves as being interested in receiving the originating computers data.

Multicasting is useful for such applications as updating the address books of mobile computer users in the field, sending out newsletters to a distribution list, and broadcasting streaming media to an audience that has tuned into the event by setting up multicast group membership.

In effect, IGMP Snooping manages multicast traffic by making use of switches, routers, and hosts that support IGMP. Enabling IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the switch. IGMP has three fundamental types of messages, as shown below:

Message	Description
Query	A message sent from the querier (an IGMP router or a switch) which asks for a response from each host that belongs to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit as a member of a specific multicast group.

You can enable **IGMP Snooping** and **IGMP Query** functions here. You will see the information of the IGMP Snooping function in this section, including different multicast groups' VID and member ports, and IP multicast addresses that range from 224.0.0.0 to 239.255.255.255.

In this section, Force filtering can determined whether the switch flooding unknown multicast traffic or not.

Following commands are included in this section:

4.8.1 IGMP Snooping

4.8.2 IGMP Query

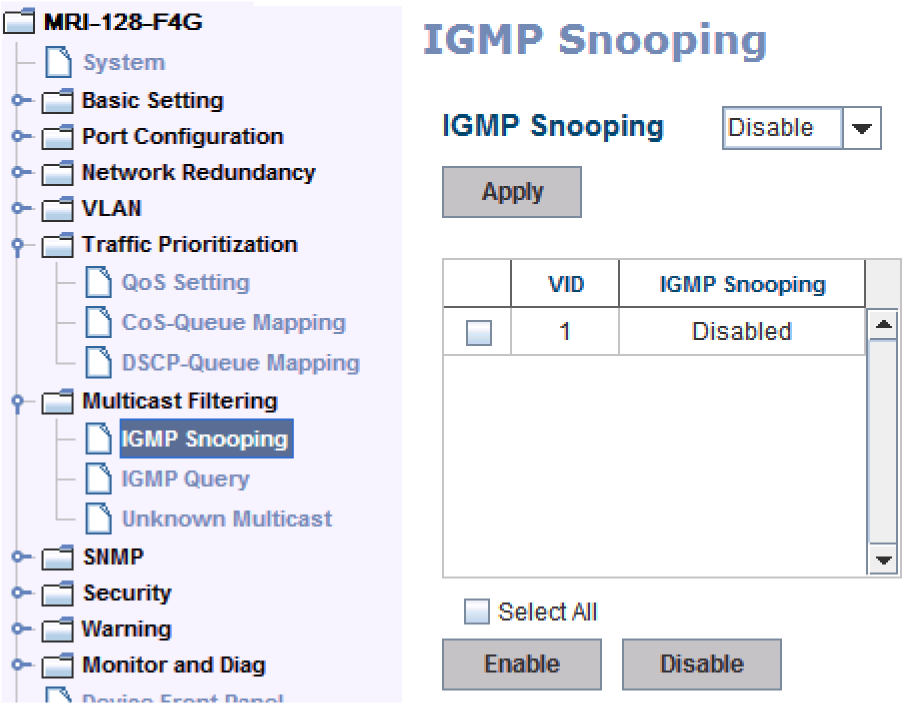
4.8.3 Unknown multicast

4.8.4 GMRP

4.8.5 CLI Commands of the Multicast Filtering

4.8.1 IGMP Snooping

This page is to enable IGMP Snooping feature, assign IGMP Snooping for specific VLAN, and view IGMP Snooping table from dynamic learnt or static manual key-in. The switch support IGMP snooping V1/V2/V3 automatically and IGMP query V1/V2.



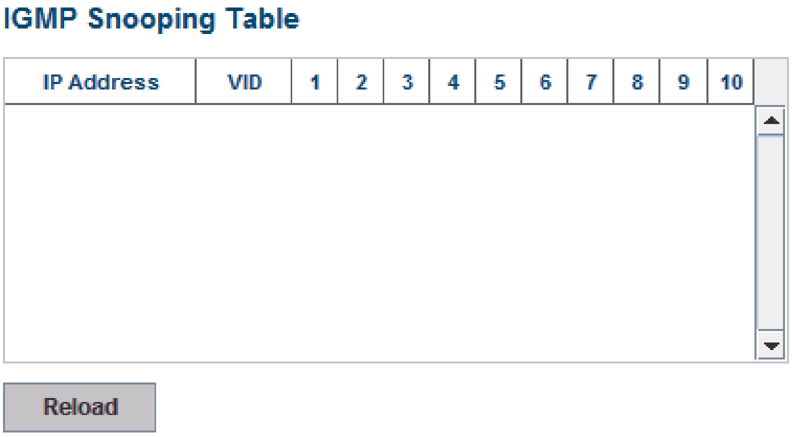
IGMP Snooping: Disable

	VID	IGMP Snooping
□	1	Disabled

□ Select All

IGMP Snooping, you can select **Enable** or **Disable** here. After enabling IGMP Snooping, you can then enable IGMP Snooping for specific VLAN. You can enable IGMP Snooping for some VLANs so that some of the VLANs will support IGMP Snooping and others won't.

To assign IGMP Snooping to VLAN, please select the **checkbox** of VLAN ID or select **Select All** checkbox for all VLANs. Then press **Enable**. In the same way, you can also **Disable** IGMP Snooping for certain VLANs.



IGMP Snooping Table

IP Address	VID	1	2	3	4	5	6	7	8	9	10

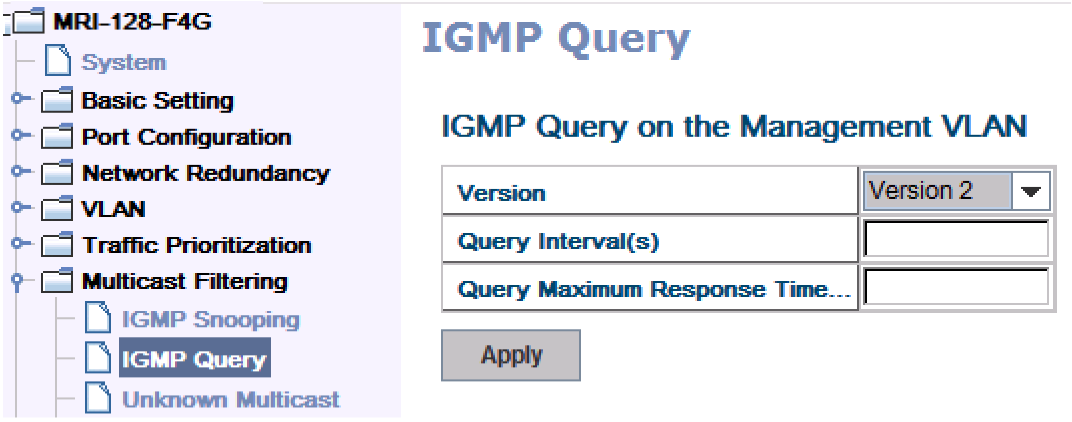
IGMP Snooping Table: In the table, you can see multicast group IP address, VLAN ID it belongs to, and member ports of the multicast group. the switch supports 256 multicast groups. Click on **Reload** to refresh the table.

4.8.2 IGMP Query

This page allows users to configure **IGMP Query** feature. Since the switch can only be configured by member ports of the management VLAN, IGMP Query can only be enabled on the management VLAN. If you want to run IGMP Snooping feature in several VLANs, you should notice that whether each VLAN has its own IGMP Querier first.

The IGMP querier periodically sends query packets to all end-stations on the LANs or VLANs that are connected to it. For networks with more than one IGMP querier, a switch with the lowest IP address will become the IGMP querier.

In IGMP Query selection, you can select V1, V2 or Disable. **V1** means IGMP V1 General Query and **V2** means IGMP V2 General Query. The query will be forwarded to all multicast groups in the VLAN. **Disable** allows you to disable IGMP Query.



IGMP Query

IGMP Query on the Management VLAN

Version	Version 2
Query Interval(s)	
Query Maximum Response Time...	

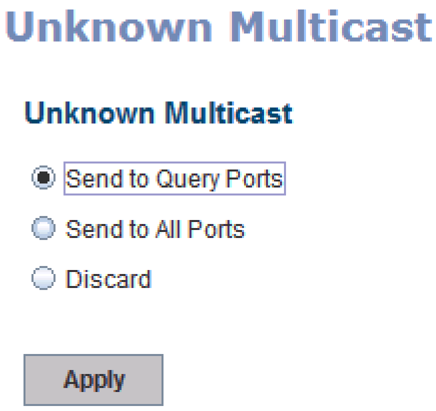
Query Interval(s): The period of query sent by querier.

Query Maximum Response Time: The span querier detect to confirm there are no more directly connected group members on a LAN.

Once you finish configuring the settings, click on **Apply** to apply your configuration.

4.8.3 Unknown Multicast

This page allows you to decide how to forward the unknown multicast traffic. After enabled IGMP Snooping, the known multicast can be filtered by IGMP Snooping mechanism and forwarded to the member ports of the known multicast groups. The other multicast streams which are not leant is so-called unknown multicast, the switch decide how to forward them based on the setting of this page.



Unknown Multicast

Unknown Multicast

● Send to Query Ports

○ Send to All Ports

○ Discard

Send to Query Ports: The unknown multicast will be sent to the Query ports. The Query port means the port received the IGMP Query packets and it is usually the uplink port on the switch.

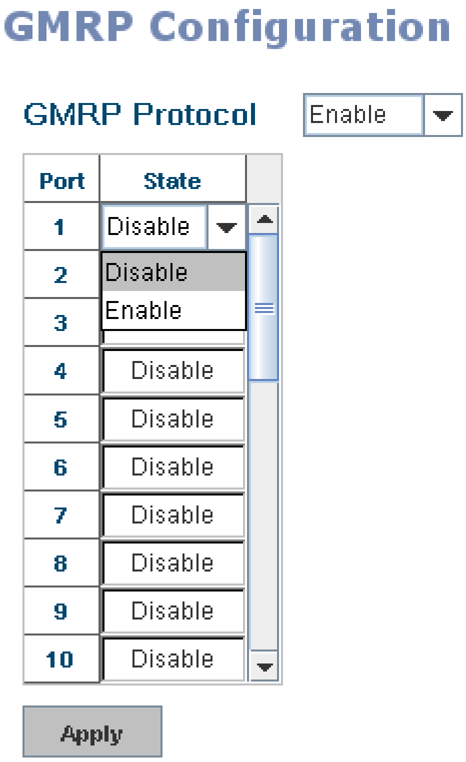
Send to All Ports: The unknown multicast will be flooded to all ports even if they are not member ports of the groups.

Discard: The unknown multicast will be discarded. Non-member ports will not receive the unknown multicast streams.

Once you finish configuring the settings, click on **Apply** to apply your configuration.

4.8.4 GMRP

To enable the GMRP configuration, the Global GMRP Configuration should be enabled first. And all the port interfaces should enable GMRP learning as well. Then the switch exchanges the IGMP Table with other switches which is also GMRP-aware devices.



GMRP Configuration

GMRP Protocol: Enable

Port	State
1	Disable
2	Disable
3	Enable
4	Disable
5	Disable
6	Disable
7	Disable
8	Disable
9	Disable
10	Disable

4.8.5 CLI Commands of the Multicast Filtering

Command Lines of the multicast filtering configuration

Feature	Command Line
IGMP Snooping	
IGMP Snooping - Global	Switch(config)# ip igmp snooping IGMP snooping is enabled globally. Please specify on which vlans IGMP snooping enables Switch(config)# ip igmp snooping <?> immediate-leave leave group when receive a leave message last-member-query-interval the interval for which

	the switch waits before updating the table entry source-only-learning Source-Only-Learning vlan Virtual LAN
IGMP Snooping - VLAN	Switch(config)# ip igmp snooping vlan VLANLIST allowed vlan list all all existed vlan Switch(config)# ip igmp snooping vlan 1-2 IGMP snooping is enabled on vlan 1 IGMP snooping is enabled on vlan 2
Disable IGMP Snooping - Global	Switch(config)# no ip igmp snoopin IGMP snooping is disabled globally ok.
Disable IGMP Snooping - VLAN	Switch(config)# no ip igmp snooping vlan 3 IGMP snooping is disabled on VLAN 3.
Display – IGMP Snooping Setting	Switch# sh ip igmp interface vlan1 enabled: Yes version: IGMPv1 query-interval; 125s query-max-response-time: 10s Switch# sh ip igmp snooping IGMP snooping is globally enabled Vlan1 is IGMP snooping enabled immediate-leave is disabled last-member-query-interval is 100 centiseconds Vlan2 is IGMP snooping enabled immediate-leave is disabled last-member-query-interval is 100 centiseconds Vlan3 is IGMP snooping disabled immediate-leave is disabled last-member-query-interval is 100 centiseconds
Display – IGMP Table	Switch# sh ip igmp snooping multicast all VLAN IP Address Type Ports ---- --------------- ------- ------------------------ 1 239.192.8.0 IGMP fa6, 1 239.255.255.250 IGMP fa6,
IGMP Query	

IGMP Query V1	Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# ip igmp v1
IGMP Query V2	Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# ip igmp
IGMP Query version	Switch(config-if)# ip igmp version 1 Switch(config-if)# ip igmp version 2
Disable	Switch(config)# int vlan 1 Switch(config-if)# no ip igmp
Display	Switch# sh ip igmp interface vlan1 enabled: Yes version: IGMPv2 query-interval: 125s query-max-response-time: 10s Switch# show running-config …. ! interface vlan1 ip address 192.168.2.200/24 ip igmp no shutdown ! …….
Unknown Multicast	
Send to Query Ports –	Switch(config)# ip igmp snooping source-only-learning IGMP Snooping Source-Only-Learning enabled
Discard (Force filtering)	Switch(config)# mac-address-table multicast filtering Filtering unknown multicast addresses ok!
Send to All Ports (No Discard, No Send to Query Ports)	Switch(config)# no mac-address-table multicast filtering Switch(config)# no ip igmp snooping source-only-learning IGMP Snooping Source-Only-Learning disabled

4.9 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices and is a member of the TCP/IP protocol suite. The switch support SNMP v1 and v2c and V3.

An SNMP managed network consists of two main components: agents and a manager. An agent is a management software module that resides in a managed switch. An agent translates the local management information from the managed device into a SNMP compatible format. The manager is the console through the network.

Following commands are included in this chapter:

4.9.1 SNMP Configuration

This page allows users to configure SNMP V1/V2c Community. The community string can be viewed as the password because SNMP V1/V2c doesn’t request you to enter password before you try to access SNMP agent.

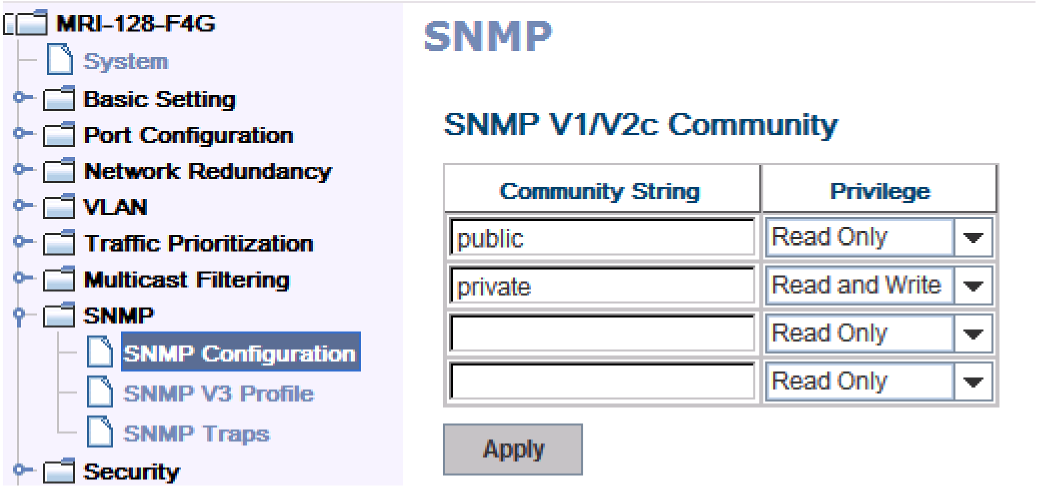
The community includes two privileges, Read Only and Read and Write.

With **Read Only** privilege, you only have the ability to read the values of MIB tables. Default community string is Public.

With **Read and Write** privilege, you have the ability to read and set the values of MIB tables. Default community string is Private.

The switch allows users to assign four community strings. Type the community string and select the privilege and then press **Apply**.

Note: *When you first install the device in your network, we highly recommend you to change the community string. Since most SNMP management application uses Public and Private as their default community name, this might be the leakage of the network security.*



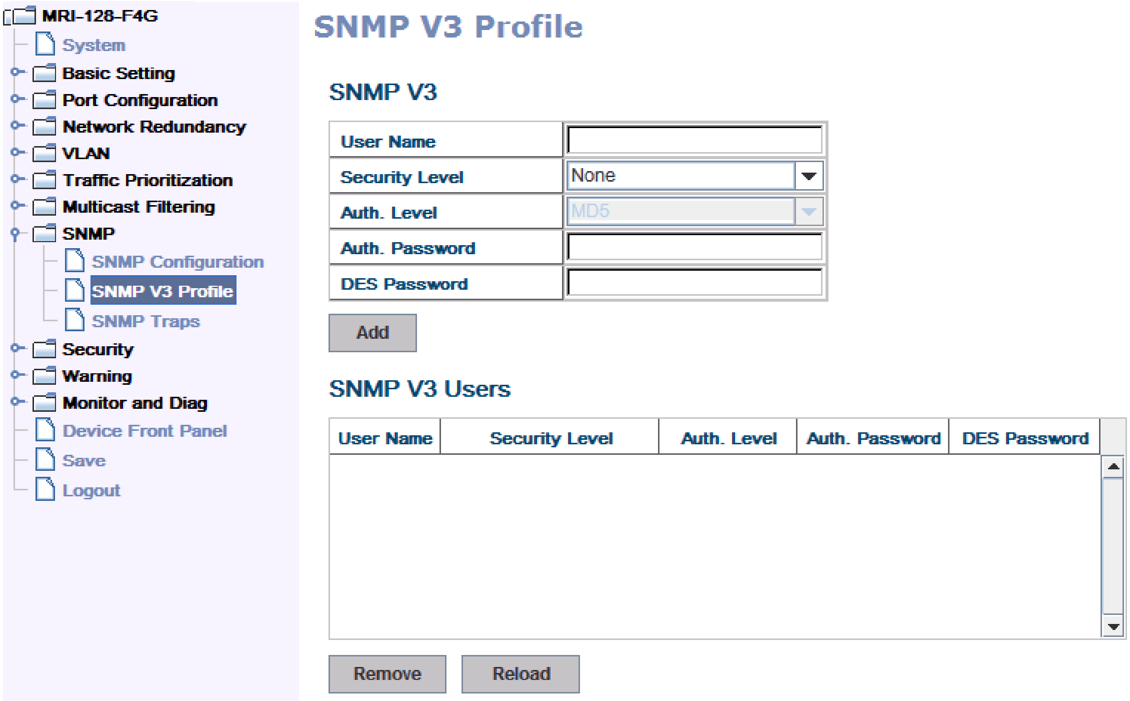
SNMP

SNMP V1/V2c Community

Community String	Privilege
public	Read Only
private	Read and Write
	Read Only
	Read Only

4.9.2 SNMP V3 Profile

SNMP V3 can provide more security functions when the user performs remote management through SNMP protocol. It delivers SNMP information to the administrator with user authentication; all of data between the switch and the administrator are encrypted to ensure secure communication.



SNMP V3 Profile

SNMP V3

User Name	
Security Level	None
Auth. Level	MD5
Auth. Password	
DES Password	

SNMP V3 Users

User Name	Security Level	Auth. Level	Auth. Password	DES Password

Security Level: Here the user can select the following levels of security: None, User Authentication, and Authentication with privacy.

Authentication Protocol: Here the user can select either MD5 (Message-Digest algorithm 5) or SHA (Secure Hash Algorithm). MD5 is a widely used cryptographic hash function with a 128-bit hash value. SHA (Secure Hash Algorithm) hash functions refer to five Federal Information Processing Standard-approved algorithms for computing a condensed digital representation. The switch provides two user authentication protocols in MD5 and SHA. You will need to configure SNMP v3 parameters for your SNMP tool with the same authentication method.

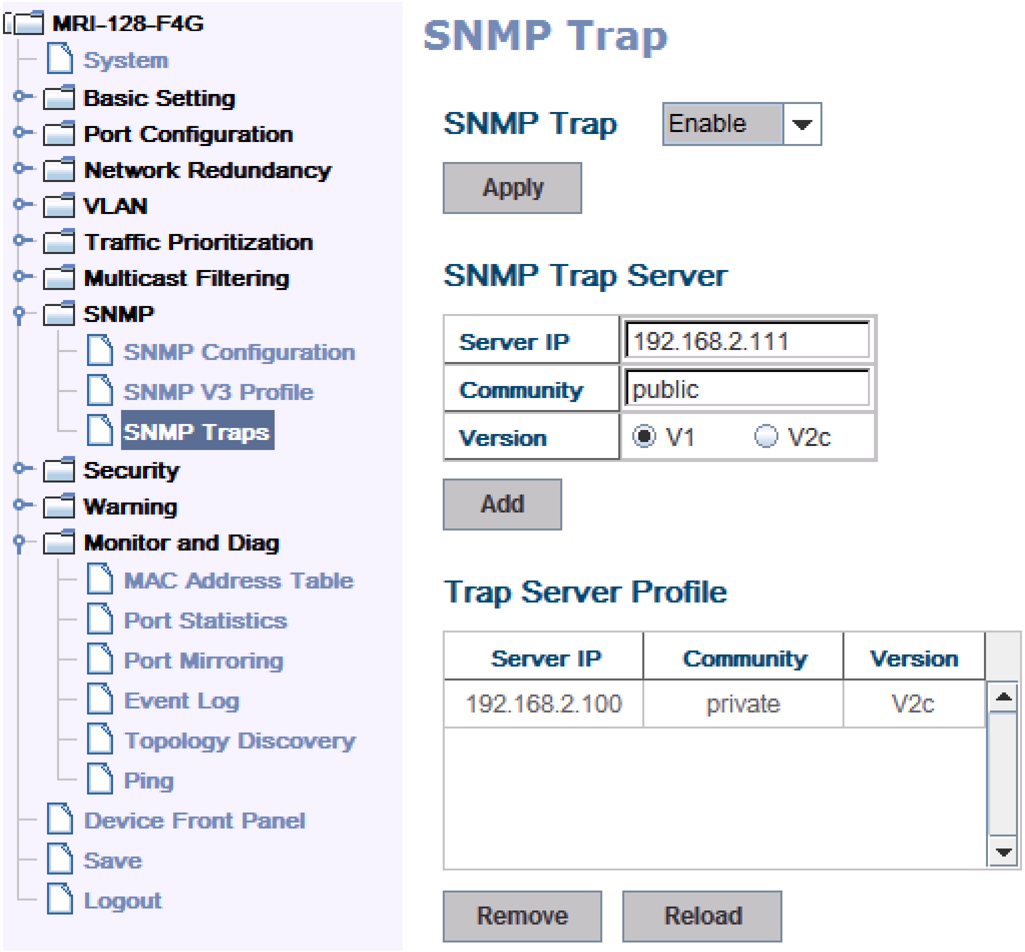
Authentication Password: Here the user enters the SNMP v3 user authentication password.

DES Encryption Password: Here the user enters the password for SNMP v3 user DES Encryption.

4.9.3 SNMP Traps

SNMP Trap is the notification feature defined by SNMP protocol. All the SNMP management applications can understand such trap information. So you don't need to install new application to read the notification information.

This page allows users to **Enable SNMP Trap,** configure the **SNMP Trap server IP**, **Community** name, and trap **Version V1 or V2**. After configuration, you can see the change of the SNMP pre-defined standard traps and Westermo pre-defined traps. The pre-defined traps can be found in Westermo private MIB.



SNMP Trap: Enable

SNMP Trap Server

Server IP	192.168.2.111
Community	public
Version	● V1 ○ V2c

Trap Server Profile

Server IP	Community	Version
192.168.2.100	private	V2c

4.9.4 CLI Commands of the SNMP

Command Lines of the SNMP configuration

Feature	Command Line
SNMP Community	
Read Only Community	Switch(config)# snmp-server community public ro community string add ok
Read Write Community	Switch(config)# snmp-server community private rw community string add ok
SNMP Trap	
Enable Trap	Switch(config)# snmp-server enable trap Set SNMP trap enable ok.
SNMP Trap Server IP without specific community name	Switch(config)# snmp-server host 192.168.2.33 SNMP trap host add OK.
SNMP Trap Server IP with version 1 and community	Switch(config)# snmp-server host 192.168.2.33 version 1 private SNMP trap host add OK. ***Note: private is the community name, version 1 is the SNMP version***
SNMP Trap Server IP with version 2 and community	Switch(config)# snmp-server host 192.168.2.33 version 2 private SNMP trap host add OK.
Disable SNMP Trap	Switch(config)# no snmp-server enable trap Set SNMP trap disable ok.
Display	Switch# sh snmp-server trap SNMP trap: Enabled SNMP trap community: public Switch# show running-config .... snmp-server community public ro snmp-server community private rw snmp-server enable trap snmp-server host 192.168.2.33 version 2 admin snmp-server host 192.168.2.33 version 1 admin ....

4.10 Security

The switch provides several security features for you to secure your connection. The Filter Set is also known as Access Control List. The ACL feature includes traditional Port Security and IP Security.

Following commands are included in this section:

4.10.1 Filter Set (Access Control List)

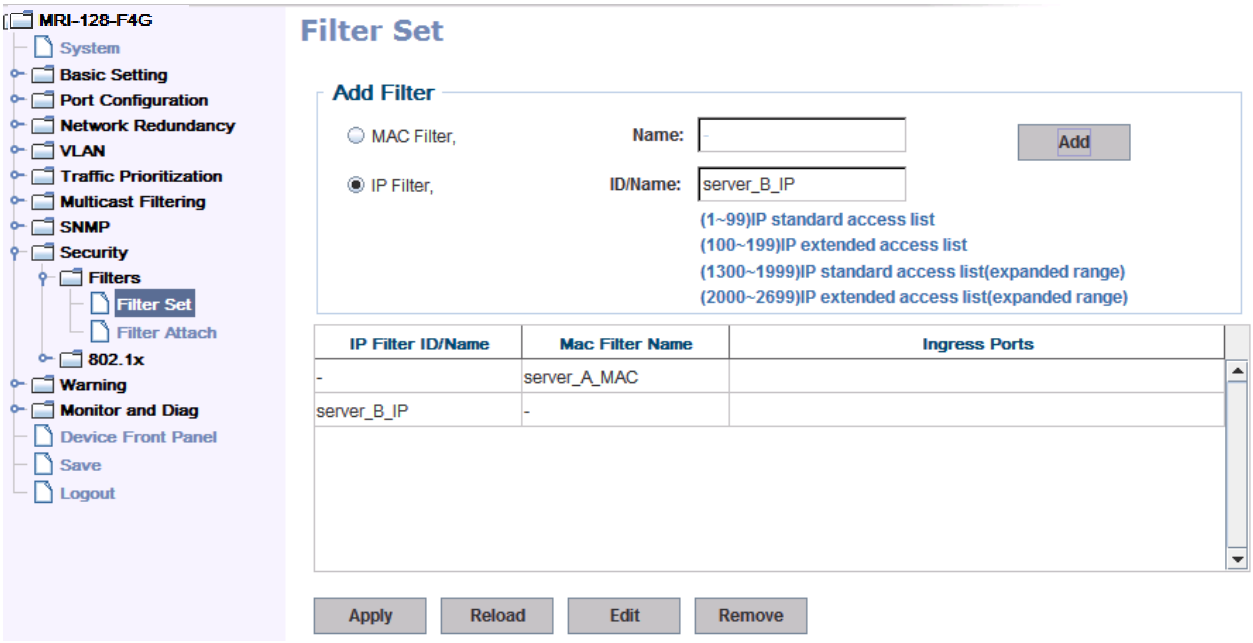
4.10.2 IEEE 802.1x

4.10.3 CLI Commands of the Security

4.10.1 Filter Set (Access Control List)

The Filter Set is known as Access Control List feature. There are two major types, one is MAC Filter and the one is IP Filter.

ACE is short of Access Control Entry, user defines the Permit or Deny rule for specific IP/MAC address or IP groups by network mask in each ACE. One ACL may include several ACEs, the system checks the ACEs one after one and forward based on the result. Once the rules conflict, the old entry is selected as the forward rule.



Filter Set

Add Filter

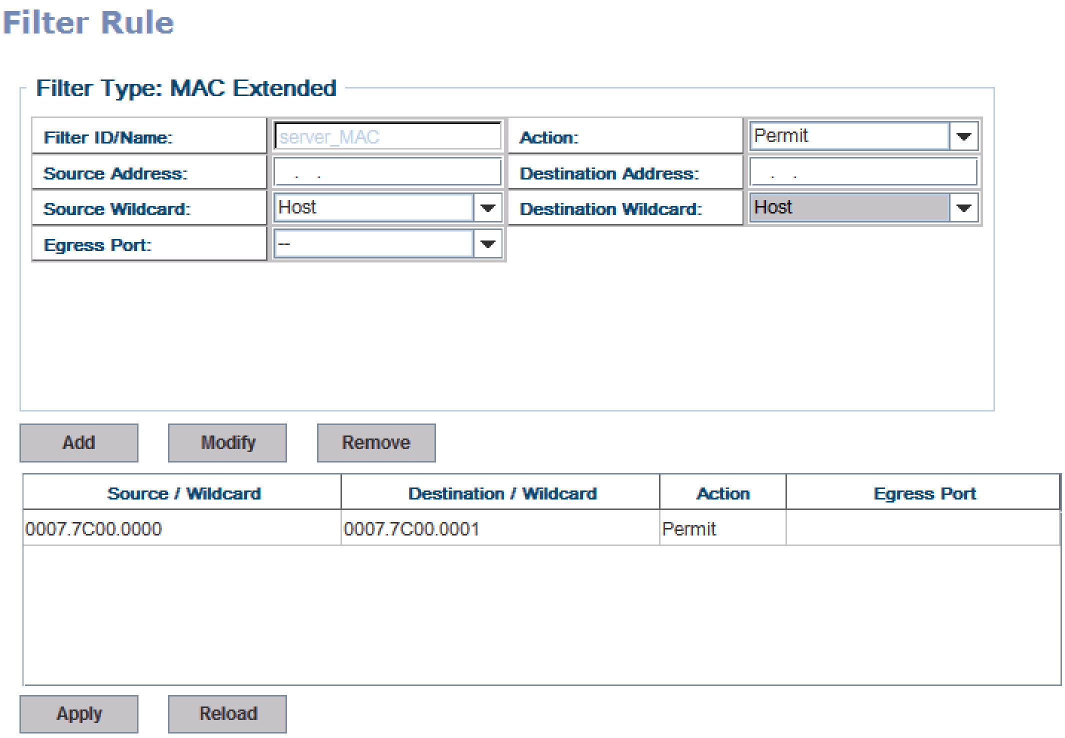
○ MAC Filter, Name:

● IP Filter, ID/Name: server_B_IP

(1~99)IP standard access list
(100~199)IP extended access list
(1300~1999)IP standard access list(expanded range)
(2000~2699)IP extended access list(expanded range)

IP Filter ID/Name	Mac Filter Name	Ingress Ports
-	server_A_MAC	
server_B_IP	-	

Type the **Name** when select **MAC Filter**, type **ID/Name** when select **IP Filter**. The ID for IP access list is listed as below of the field. Click **Add** to add the rule. Click **Edit** to edit the content for the rule. After configured, click **Apply** to apply all the rules. **Reload** to reload setting. **Remove** to remove one of the entries.



Filter Rule

Filter Type: MAC Extended

Filter ID/Name:	server_MAC	Action:	Permit
Source Address:	. .	Destination Address:	. .
Source Wildcard:	Host	Destination Wildcard:	Host
Egress Port:	--		

Source / Wildcard	Destination / Wildcard	Action	Egress Port
0007.7C00.0000	0007.7C00.0001	Permit	

MAC Filter (Port Security):

The MAC Filter allows user to define the Access Control List for specific MAC address or a group of MAC addresses.

Filter ID/Name: The name for this MAC Filter entry.

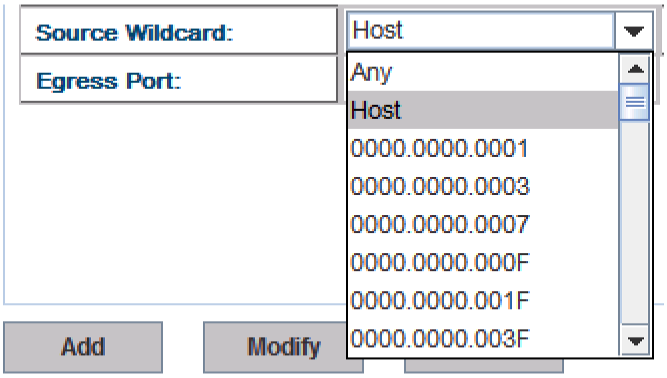
Action: Permit to permit traffic from specified sources.

Deny to deny traffic from those sources.

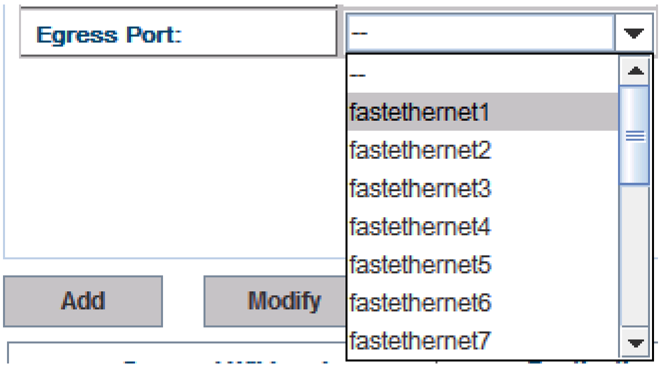
Source/Destination Address: Type the MAC address you want configure, the format is "AABB.CCDD.EEFF". Example: "Source to Destination" is "0007.7c00.0000 to 0007.7c00.0002".

Source/Destination Wildcard: This command allows user to define single host or a group of hosts based on the wildcard. Some of the allowance examples are as below:

Wildcard	Bit	Number of allowance	Note
Any	1111.1111.1111	All	
Host		1	Only the Source or Destination.
0000.0000.0003	0000.0000.000(00000011)	3	
0000.0000.0007	0000.0000.000(00000111)	7	
0000.0000.000F	0000.0000.000(11111111)	15	



Egress Port: Bind the MAC Filter rule to specific front port.

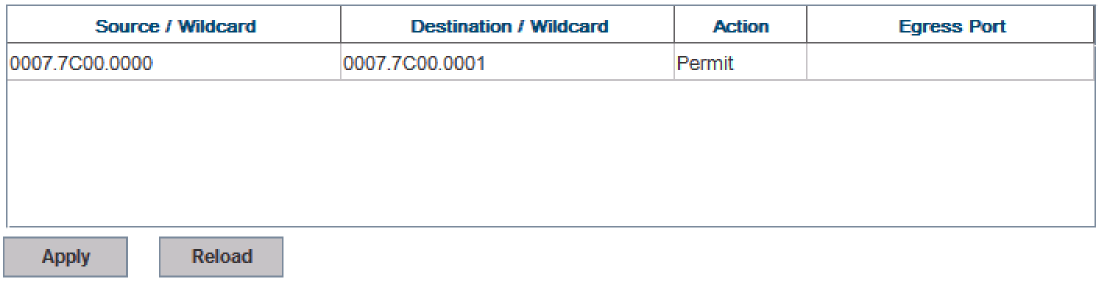


Once you finish configuring the ACE settings, click on **Add** to apply your configuration. You can see below screen is shown.

Example of the below Entry:

Permit Source MAC “0007.7c00.0000” to Destination MAC “0007.7c00.0002”.

The Permit rule is egress rule and it is bind to Gigabit Ethernet Port 25.



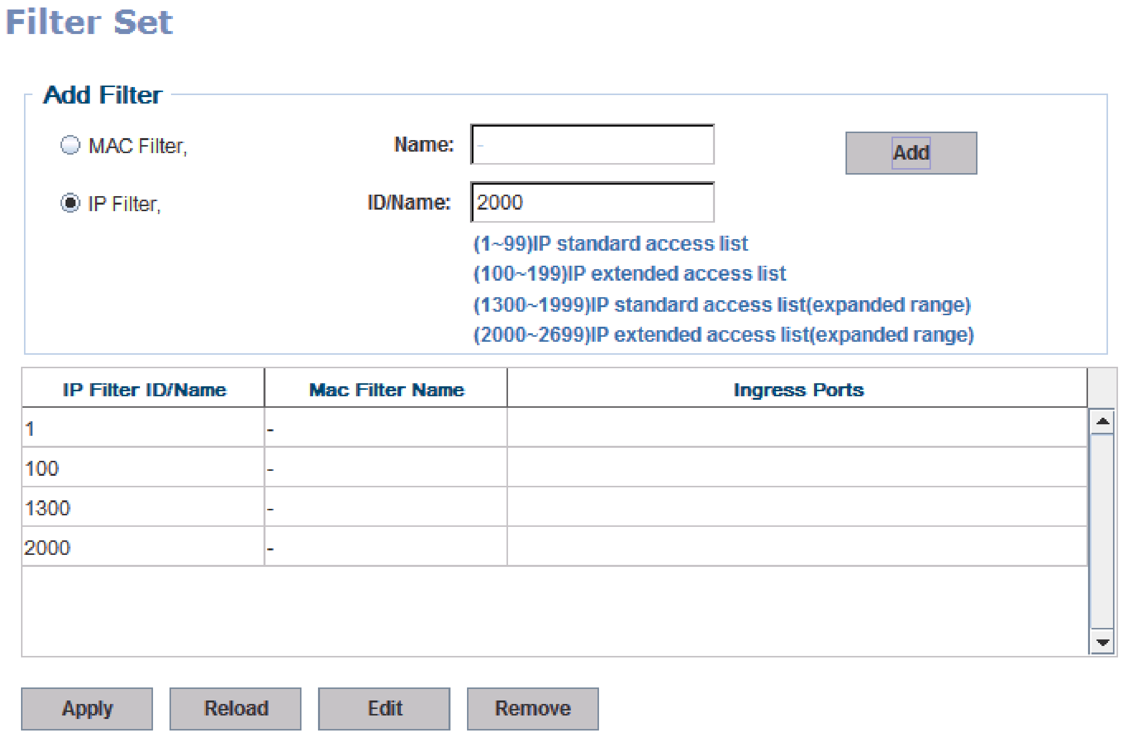
Source / Wildcard	Destination / Wildcard	Action	Egress Port
0007.7C00.0000	0007.7C00.0001	Permit	

Once you finish configuring the settings, click on **Apply** to apply your configuration.

IP Filter:

Type **ID/Name** when select **IP Filter**. The ID for IP access list is listed as below of the field. You can also type ACL name in this field, it goes to IP Extended mode setting and support both IP Standard and IP Extended mode depend on the setting. Click **Add** to add the rule. Click **Edit** to edit the content for the rule. After configured, click **Apply** to apply all the rules. **Reload** to reload setting. **Remove** to remove one of the entries.

Example:



Filter Set

Add Filter

○ MAC Filter, Name: -

● IP Filter, ID/Name: 2000

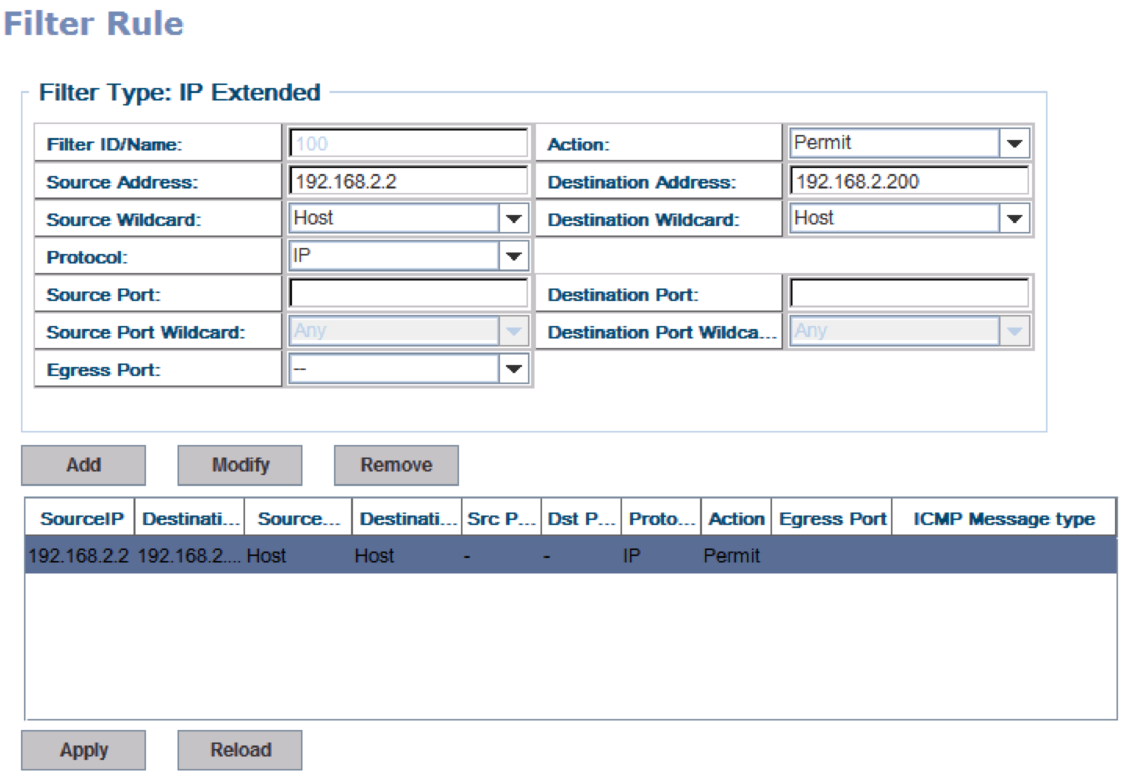
(1~99)IP standard access list
(100~199)IP extended access list
(1300~1999)IP standard access list(expanded range)
(2000~2699)IP extended access list(expanded range)

IP Filter ID/Name	Mac Filter Name	Ingress Ports
1	-	
100	-	
1300	-	
2000	-	

IP Standard Access List: This kind of ACL allows user to define filter rules according to the source IP address.

IP Extended Access List: This kind of ACL allows user to define filter rules according to the source IP address, destination IP address, Source TCP/UDP port, destination TCP/UDP port and ICMP type and code.

Click **Edit** to configure the IP Filter Rules.



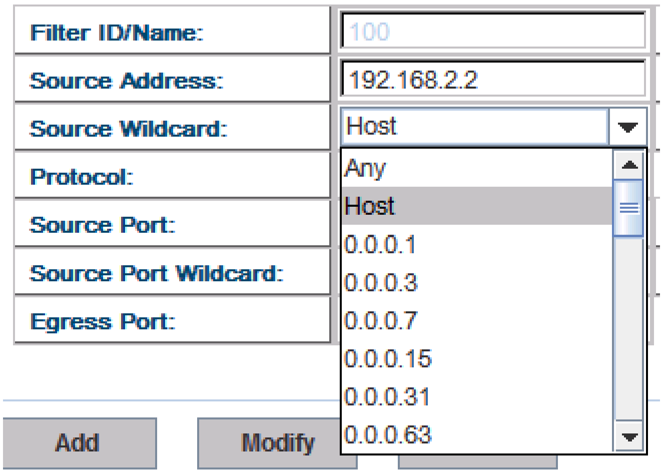
Filter ID/Name:	100	Action:	Permit
Source Address:	192.168.2.2	Destination Address:	192.168.2.200
Source Wildcard:	Host	Destination Wildcard:	Host
Protocol:	IP		
Source Port:		Destination Port:	
Source Port Wildcard:	Any	Destination Port Wildca...	Any
Egress Port:	--		

SourceIP	Destinati...	Source...	Destinati...	Src P...	Dst P...	Proto...	Action	Egress Port	ICMP Message type
192.168.2.2	192.168.2....	Host	Host	-	-	IP	Permit		

Filter ID/Name: The ID or the name for this IP Filter entry.

Action: Permit to permit traffic from specified sources. **Deny** to deny traffic from those sources.

Source/Destination Address: Type the source/destination IP address you want configure.



Filter ID/Name:	100
Source Address:	192.168.2.2
Source Wildcard:	Host
Protocol:	
Source Port:	
Source Port Wildcard:	
Egress Port:	

Source/Destination Wildcard: This command allows user to define single host or a group of hosts based on the wildcard. Some of the allowance examples are as below:

Wildcard	Bit	Number of allowance	Note
Any	11111111.11111111. 11111111.11111111	All	All IP addresses. Or a mask: 255.255.255.255
Host	0.0.0.0	1	Only the Source or Destination host.
0.0.0.3	0.0.0.(00000011)	3	
0.0.0.7	0.0.0.(00000111)	7	
0.0.0.15	0.0.0.(11111111)	15	
….			

Note: The mask is a wildcard mask: the high-order bits of the mask that are binary zeros determine how many corresponding high-order bits in the IP address are significant. The selected action applies to any source address with these high-order bits.

Protocol: Select a protocol you want associate with the filter. The field includes IP, TCP, UDP or ICMP type.

Destination Port: TCP/UDP port of the Destination Port field.

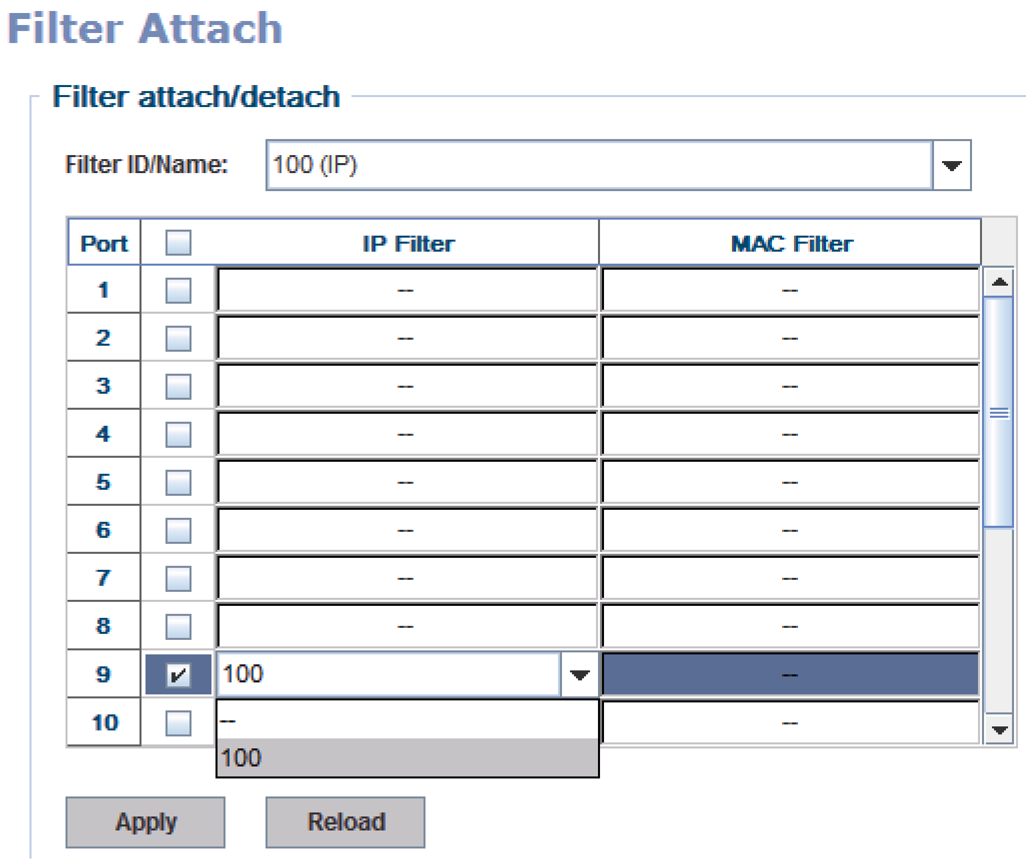
ICMP Type: The ICMP Protocol Type range from 1 ~ 255.

ICMP Code: The ICMP Protocol Code range from 1 ~ 255.

Egress Port: Bind this Filter to selected egress port.

Click the **Add** button to add the rule to the Filter. Click the **Remove** button to remove the selected rule from Filter. Click the **Modify** button to edit the rule which you selected. Click the **Reload** button to reload the rule table.

Click the **Apply** button to apply the Filter configurations.



Filter Attach

Filter attach/detach

Filter ID/Name: 100 (IP)

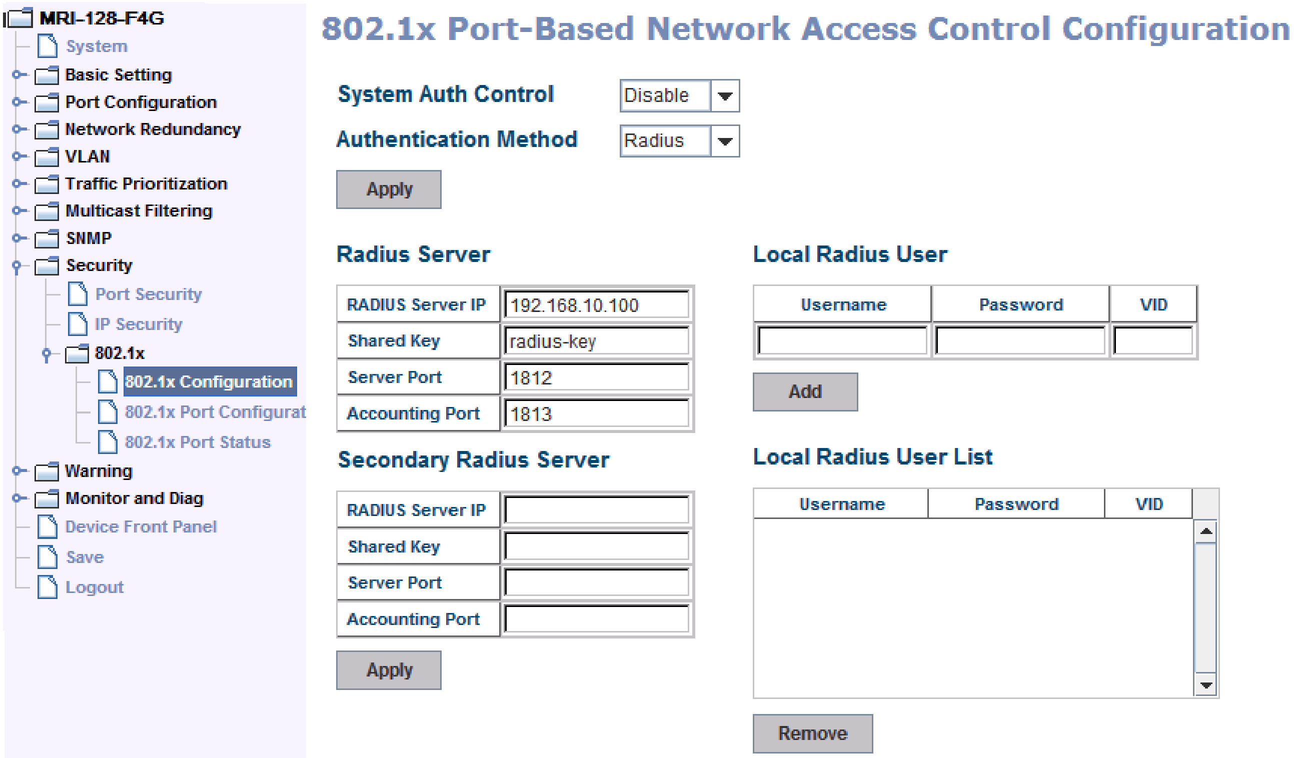
Port	□	IP Filter	MAC Filter
1	□	--	--
2	□	--	--
3	□	--	--
4	□	--	--
5	□	--	--
6	□	--	--
7	□	--	--
8	□	--	--
9	☑	100	--
10	□	-- 100	--

After configured the ACL filter rules, remember associate this filter with the physical ports. Then the port has the capability to filter traffic/attach based on the packets lost.

4.10.2 IEEE 802.1x

802.1X configuration

IEEE 802.1X is the protocol that performing authentication to obtain access to IEEE 802 LANs. It is port-base network access control and the switch could control which connection should be available or not.



802.1x Port-Based Network Access Control Configuration

System Auth Control: Disable

Authentication Method: Radius

Radius Server

RADIUS Server IP	192.168.10.100
Shared Key	radius-key
Server Port	1812
Accounting Port	1813

Secondary Radius Server

RADIUS Server IP	
Shared Key	
Server Port	
Accounting Port	

Local Radius User

Username	Password	VID

Local Radius User List

Username	Password	VID

System Auth Control: To enable or disable the 802.1x authentication.

Authentication Method: Radius is an authentication server that provides key for authentication, with this method user must connect the switch to the Radius server. If user selects Local for the authentication method, the switch will use the local user data base which can be created in this page for authentication.

Radius Server IP: The IP address of the Radius server

Shared Key: The password for communicate between switch and Radius Server.

Server Port: UDP port of the Radius server.

Accounting Port: Port for packets that contain the information of account login or logout.

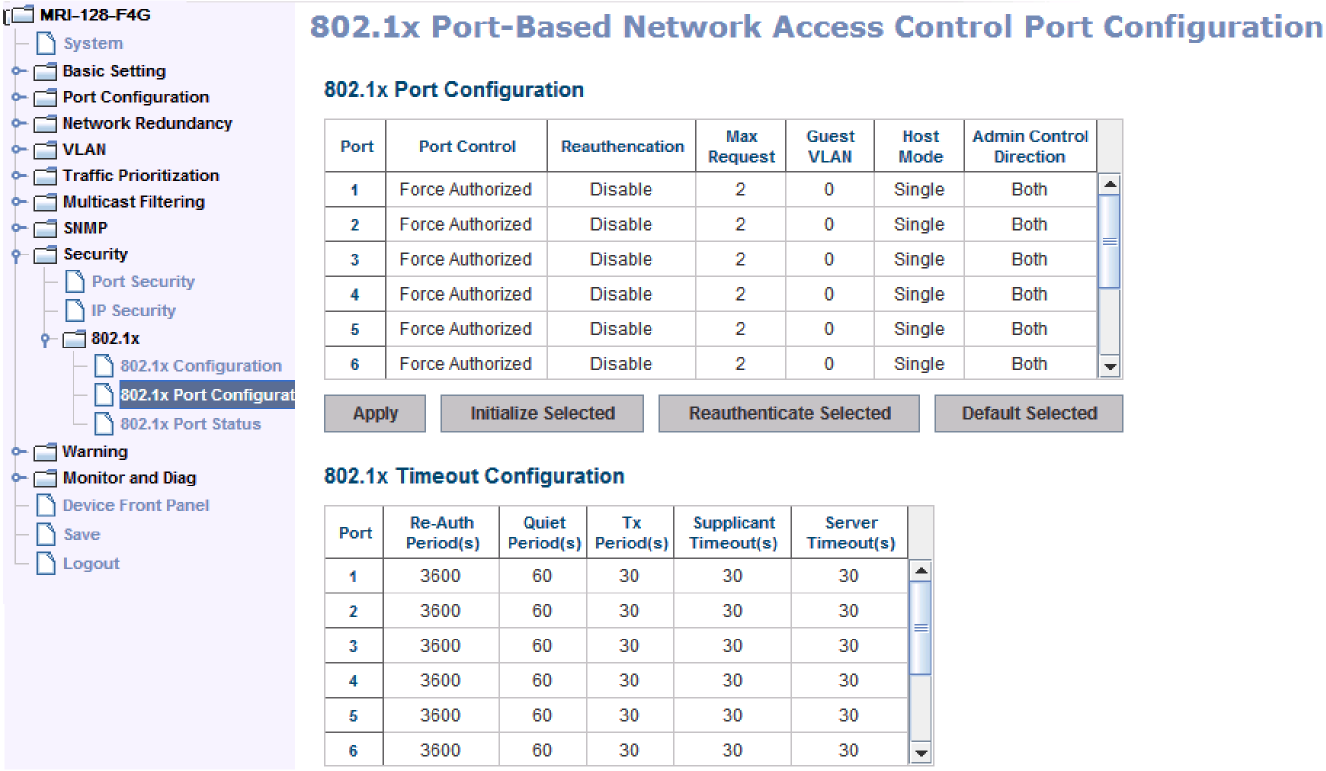
Secondary Radius Server IP: Secondary Radius Server could be set in case of the primary radius server down.

Local Radius User: The user can add Account/Password for local authentication.

Local Radius User List: This is a list shows the account information; user also can remove selected account.

802.1x Port Configuration

After the configuration of Radius Server or Local user list, user also need configure the authentication mode, authentication behavior, applied VLAN for each port and permitted communication. The following information will explain the port configuration.



802.1x Port-Based Network Access Control Port Configuration

802.1x Port Configuration

Port	Port Control	Reauthencation	Max Request	Guest VLAN	Host Mode	Admin Control Direction
1	Force Authorized	Disable	2	0	Single	Both
2	Force Authorized	Disable	2	0	Single	Both
3	Force Authorized	Disable	2	0	Single	Both
4	Force Authorized	Disable	2	0	Single	Both
5	Force Authorized	Disable	2	0	Single	Both
6	Force Authorized	Disable	2	0	Single	Both

802.1x Timeout Configuration

Port	Re-Auth Period(s)	Quiet Period(s)	Tx Period(s)	Supplicant Timeout(s)	Server Timeout(s)
1	3600	60	30	30	30
2	3600	60	30	30	30
3	3600	60	30	30	30
4	3600	60	30	30	30
5	3600	60	30	30	30
6	3600	60	30	30	30

Once you finish configuring the settings, click on **Apply** to apply your configuration.

Port control: Force Authorized means this port is authorized; the data is free to in/out. Force unauthorized just opposite, the port is blocked. If users want to control this port with Radius Server, please select Auto for port control.

Reauthentication: If enable this field, switch will ask client to re-authenticate. The default time interval is 3600 seconds.

Max Request: the maximum times that the switch allow client request.

Guest VLAN: VLAN ID 0 to 4094 is available for this field. If this field is set to 0, that means the port is blocked for failed authentication. Otherwise, the port will be set to a Guest VLAN.

Host Mode: If there are more than one device connected to this port, set the Host Mode to single means only the first PC authenticate success can access this port. If this port is set to multi, all the device can access this port once any one of them pass the authentication.

Control Direction: Determined devices can end data out only or both send and receive.

Re-Auth Period: Control the Re-authentication time interval, 1~65535 is available.

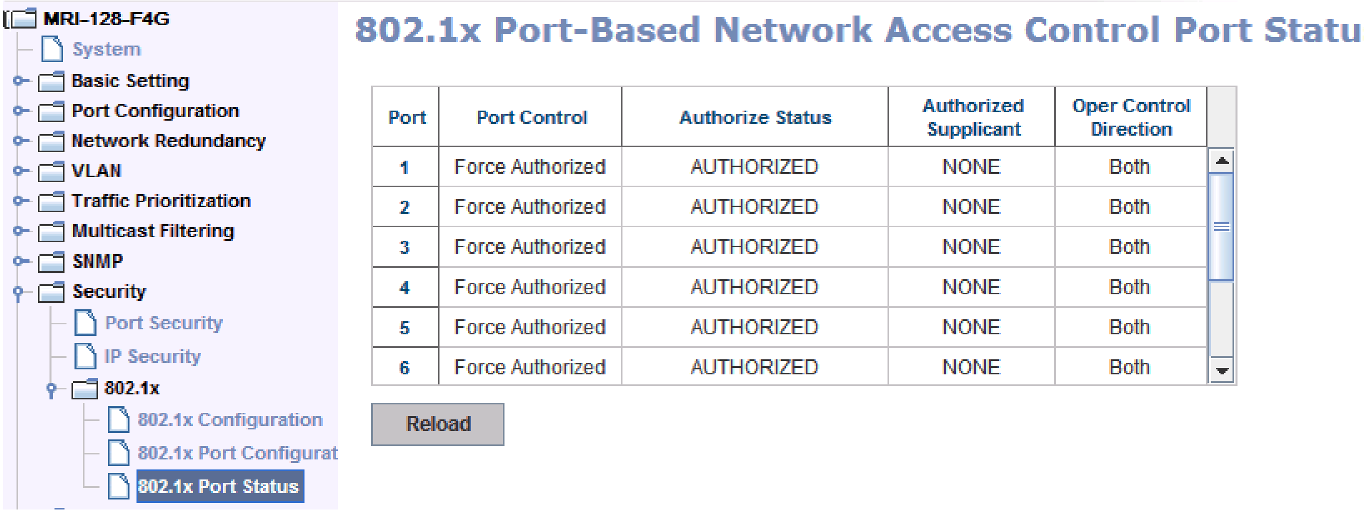
Quiet Period: When authentication failed, Switch will wait for a period and try to communicate with radius server again.

Tx period: The time interval of authentication request.
Supplicant Timeout: the timeout for the client authenticating
Sever Timeout: The timeout for server response for authenticating.

Click **Initialize Selected** to set the authorize state of selected port to initialize status.
Click **Reauthenticate Selected** to send EAP Request to supplicant to request reauthentication.
Click **Default Selected** to reset the configurable 802.1x parameters of selected port to the default values.

802.1X Port Status

The user can observe the port status for Port control, Authorize Status, Authorized Supplicant and Oper Control Direction on each port.



802.1x Port-Based Network Access Control Port Statu

Port	Port Control	Authorize Status	Authorized Supplicant	Oper Control Direction
1	Force Authorized	AUTHORIZED	NONE	Both
2	Force Authorized	AUTHORIZED	NONE	Both
3	Force Authorized	AUTHORIZED	NONE	Both
4	Force Authorized	AUTHORIZED	NONE	Both
5	Force Authorized	AUTHORIZED	NONE	Both
6	Force Authorized	AUTHORIZED	NONE	Both

4.10.3 CLI Commands of the Security

Command Lines of the Security configuration

Feature	Command Line
Port Security	
Add MAC access list	Switch(config)# mac access-list extended NAME access-list name Switch(config)# mac access-list extended server1 Switch(config-ext-macl)# permit Specify packets to forward deny Specify packets to reject end End current mode and change to enable

	mode exit Exit current mode and down to previous mode list Print command list no Negate a command or set its defaults quit Exit current mode and down to previous mode
Add IP Standard access list	Switch(config)# ip access-list extended Extended access-list standard Standard access-list Switch(config)# ip access-list standard <1-99> Standard IP access-list number <1300-1999> Standard IP access-list number (expanded range) WORD Access-list name Switch(config)# ip access-list standard 1 Switch(config-std-acl)# deny Specify packets to reject permit Specify packets to forward end End current mode and change to enable mode exit Exit current mode and down to previous mode list Print command list no Negate a command or set its defaults quit Exit current mode and down to previous mode remark Access list entry comment
Add IP Extended access list	Switch(config)# ip access-list extended <100-199> Extended IP access-list number <2000-2699> Extended IP access-list number (expanded range) WORD access-list name Switch(config)# ip access-list extended 100 Switch(config-ext-acl)# deny Specify packets to reject permit Specify packets to forward end End current mode and down to previous

	mode exit Exit current mode and down to previous mode list Print command list no Negate a command or set its defaults quit Exit current mode and down to previous mode remark Access list entry comment
Example 1: Edit MAC access list	Switch(config-ext-macl)#permit MACADDR Source MAC address xxxx.xxxx.xxxx any any source MAC address host A single source host Switch(config-ext-macl)#permit host MACADDR Source MAC address xxxx.xxxx.xxxx Switch(config-ext-macl)#permit host 0007.7c11.2233 MACADDR Destination MAC address xxxx.xxxx.xxxx any any destination MAC address host A single destination host Switch(config-ext-macl)#permit host 0007.7c11.2233 host MACADDR Destination MAC address xxxx.xxxx.xxxx Switch(config-ext-macl)#permit host 0007.7c11.2233 host 0007.7c11.2234 [IFNAME] Egress interface name Switch(config-ext-macl)#permit host 0007.7c11.2233 host 0007.7c11.2234 gi25 *Note: MAC Rule: Permit/Deny wildcard Source_MAC wildcard Dest_MAC Egress_Interface*
Example 1: Edit IP Extended access list	Switch(config)# ip access-list extended 100 Switch(config-ext-acl)#permit ip Any Internet Protocol tcp Transmission Control Protocol udp User Datagram Protocol icmp Internet Control Message Protocol Switch(config-ext-acl)#permit ip

	A.B.C.D Source address any Any source host host A single source host Switch(config-ext-acl)#permit ip 192.168.2.200 A.B.C.D Source wildcard bits Switch(config-ext-acl)#permit ip 192.168.2.200 0.0.0.1 A.B.C.D Destination address any Any destination host host A single destination host Switch(config-ext-acl)#permit ip 192.168.2.200 0.0.0.1 192.168.2.200 0.0.0.1 [IFNAME] Egress interface name Switch(config-ext-acl)#permit ip 192.168.2.200 0.0.0.1 192.168.2.200 0.0.0.1 gi26 *Note: Follow the below rule to configure ip extended access list.* *IP Rule: Permit/Deny Source_IP wildcard Dest_IP wildcard Egress_Interface* *TCP Rule: Permit/Deny tcp Source_IP wildcard Dest_IP wildcard eq Given_Port_Number Egress_Interface* *UDP Rule: Permit/Deny udp Source_IP wildcard Dest_IP wildcard eq Given_Port_Number Egress_Interface* *ICMP Rule: Permit/Deny icmp Source_IP wildcard Dest_IP wildcard ICMP_Message_Type ICMP_Message_Code Egress_Interface*
Add MAC	Switch(config)# mac-address-table static 0007.7701.0101 vlan 1 interface fa1 mac-address-table unicast static set ok!
Port Security	Switch(config)# interface fa1 Switch(config-if)# switchport port-security Disables new MAC addresses learning and aging activities! ***Note: Rule: Add the static MAC, VLAN and Port binding first, then enable the port security to stop new MAC learning.***

Disable Port Security	Switch(config-if)# no switchport port-security Enable new MAC addresses learning and aging activities!
Display	Switch# show mac-address-table static Destination Address Address Type Vlan Destination Port ------------------- --------------- ------- ------------------------ 0007.7701.0101 Static 1 fa1
802.1x (shot of dot1x)	
enable diable	Switch(config)# dot1x system-auth-control Switch(config)# Switch(config)# no dot1x system-auth-control Switch(config)#
authentic-method	Switch(config)# dot1x authentic-method local Use the local username database for authentication radius Use the Remote Authentication Dial-In User Service (RADIUS) servers for authentication Switch(config)# dot1x authentic-method radius Switch(config)#
radius server-ip	Switch(config)# dot1x radius Switch(config)# dot1x radius server-ip 192.168.2.200 key 1234 RADIUS Server Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) RADIUS Server IP : 192.168.2.200 RADIUS Server Key : 1234 RADIUS Server Port : 1812 RADIUS Accounting Port : 1813 Switch(config)#
radius server-ip	Switch(config)# dot1x radius Switch(config)# dot1x radius server-ip 192.168.2.200 key 1234 RADIUS Server Port number NOT given. (default=1812)

	RADIUS Accounting Port number NOT given. (default=1813) RADIUS Server IP : 192.168.2.200 RADIUS Server Key : 1234 RADIUS Server Port : 1812 RADIUS Accounting Port : 1813 Switch(config)#
radius secondary-server-ip	Switch(config)# dot1x radius secondary-server-ip 192.168.2.250 key 5678 Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) Secondary RADIUS Server IP : 192.168.2.250 Secondary RADIUS Server Key : 5678 Secondary RADIUS Server Port : 1812 Secondary RADIUS Accounting Port : 1813
User name/password for authentication	Switch(config)# dot1x username Westermo passwd Westermo vlan 1
Display	Switch# show dot1x <cr> all Show Dot1x information for all interface authentic-method Dot1x authentic-method interface Interface name radius Remote Access Dial-In User Service statistics Interface name username User Name in local radius database Switch# show dot1x <cr> = Switch# show dot1x all You can check all dot1x information for all interfaces. Click Ctrl + C to exit the display Switch# show dot1x interface fa1

```
Supplicant MAC ADDR <NONE>
STATE-MACHINE
                AM status : FORCE_AUTH
                BM status : IDLE
PortStatus                  : AUTHORIZED
PortControl                 : Force Authorized
Reauthentication          : Disable
MaxReq                          : 2
ReAuthPeriod                : 3600 Seconds
QuietPeriod                 : 60 Seconds
TxPeriod                        : 30 Seconds
SupplicantTimeout     : 30 Seconds
ServerTimeout              : 30 Seconds
GuestVlan                     : 0
HostMode                         : Single
operControlledDirections : Both
adminControlledDirections : Both

Switch# show dot1x radius
RADIUS Server IP       : 192.168.2.200
RADIUS Server Key     : radius-key
RADIUS Server Port : 1812
RADIUS Accounting Port : 1813
Secondary RADIUS Server IP       : N/A
Secondary RADIUS Server Key     : N/A
Secondary RADIUS Server Port : N/A
Secondary RADIUS Accounting Port : N/A

Switch# show dot1x username
802.1x Local User List
  Username : test , Password : * , VLAN ID : 1
```

4.11 Warning

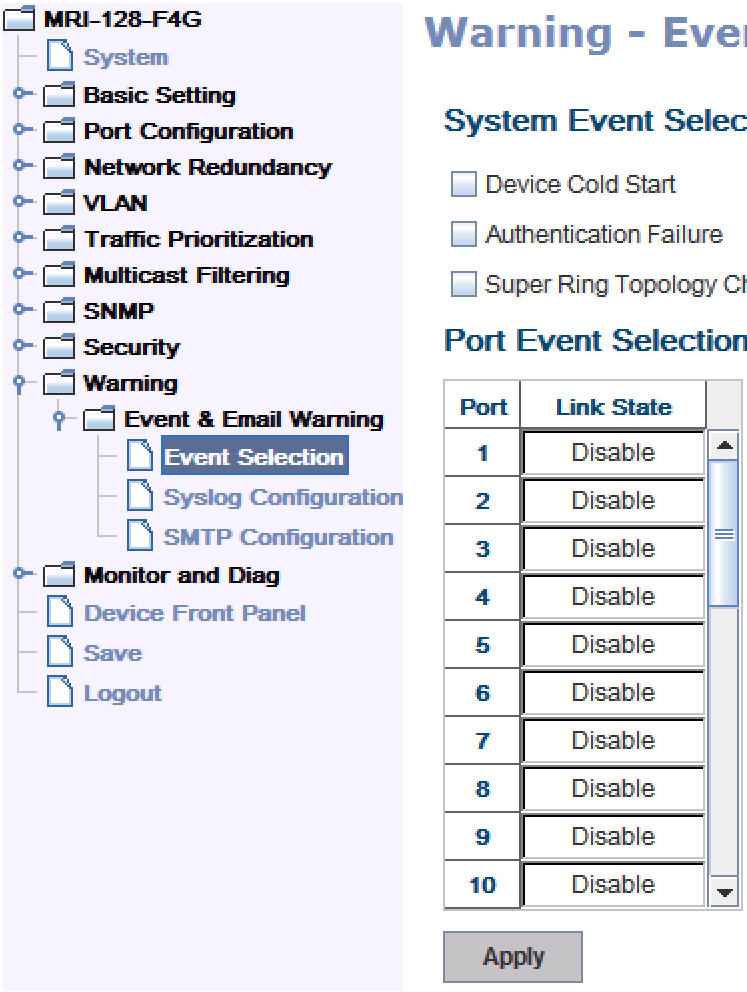
The switch provides several types of Warning features for you to remote monitor the status of end devices or the change of your network. The features include System Log and SMTP E-mail Alert.

Following commands are included in this chapter:

4.11.1 Event Selection

Event Types can be divided into two basic groups: System Events and Port Events. System Events are related to the overall function of the switch, whereas Port Events related to the activity of specific ports

System Event	**Warning Event is sent when…..**
Device Cold Start	Power is cut off and then reconnected.
Device Warm Start	Reboot the device by CLI or Web UI.
Authentication failure	An incorrect password, SNMP Community String is entered.
Time Synchronize Failure	Accessing to NTP Server is failure.
Super Ring Topology Changes	Master of Super Ring has changed or backup path is activated.
Port Event	**Warning Event is sent when…..**
Link-Up	The port is connected to another device
Link-Down	The port is disconnected (e.g. the cable is pulled out, or the opposing devices turns down)



Warning - Event Selection

System Event Selection

□ Device Cold Start □ Device Warm Start

□ Authentication Failure □ Time Synchronize Failure

□ Super Ring Topology Change

Port Event Selection

Port	Link State
1	Disable
2	Disable
3	Disable
4	Disable
5	Disable
6	Disable
7	Disable
8	Disable
9	Disable
10	Disable

Once you finish configuring the settings, click on **Apply** to apply your configuration.

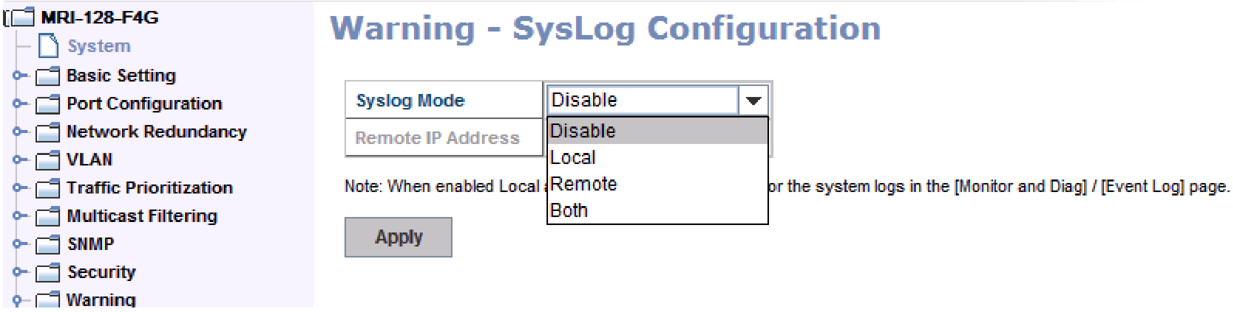
4.11.2 SysLog Configuration

System Log is useful to provide system administrator locally or remotely monitor switch events history. There are two System Log modes provided by the switch, local mode and remote mode.

Local Mode: In this mode, the switch will print the occurred events selected in the Event Selection page to System Log table of the switch. You can monitor the system logs in [Monitor and Diag] / [Event Log] page.

Remote Mode: The remote mode is also known as Server mode. In this mode, you should assign the IP address of the System Log server. The switch will send the occurred events selected in Event Selection page to System Log server you assigned.

Both: Both modes can be enabled at the same time.



Warning - SysLog Configuration

Syslog Mode	Disable
Remote IP Address	

Note: When enabled Local a or the system logs in the [Monitor and Diag] / [Event Log] page.

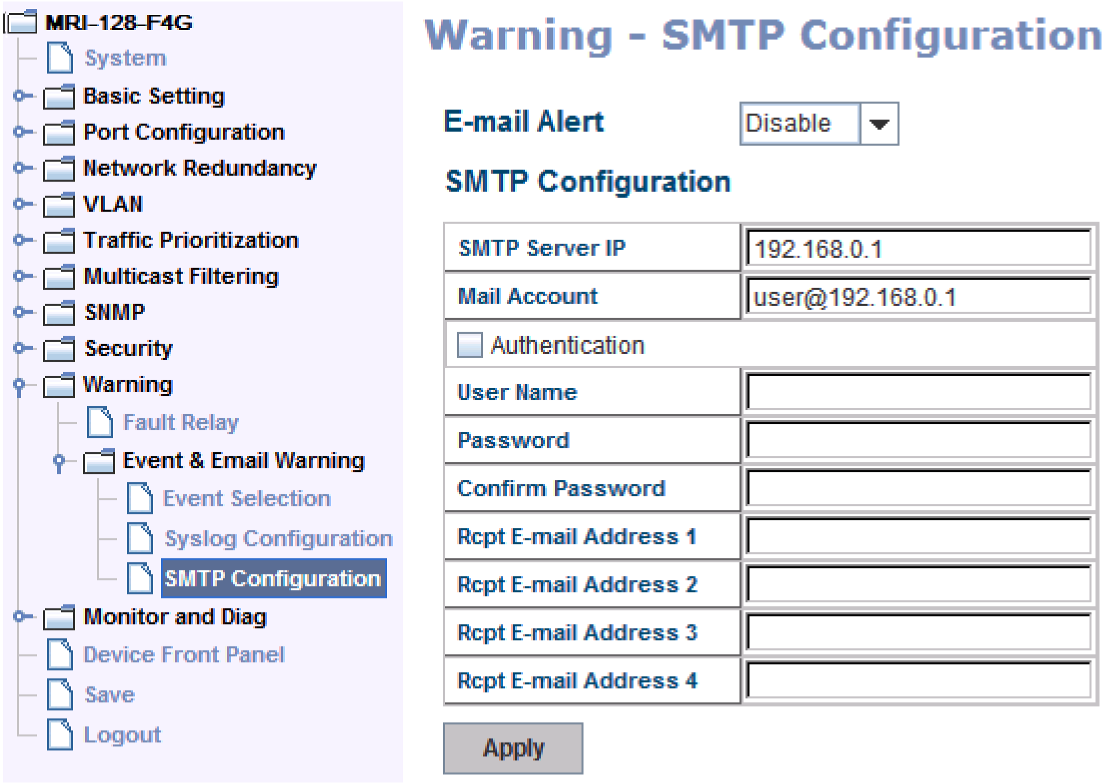
Once you finish configuring the settings, click on **Apply** to apply your configuration.

Note: *When enabling Local or Both mode, you can monitor the system logs in [Monitor and Diag] / [Event Log] page.*

4.11.3 SMTP Configuration

The switch supports E-mail Warning feature. The switch will send the occurred events to remote E-mail server. The receiver can then receive notification by E-mail. The E-mail warning is conformed to SMTP standard.

This page allows you to enable E-mail Alert, assign the SMTP Server IP, Sender E-mail, and Receiver E-mail. If SMTP server requests you to authorize first, you can also set up the username and password in this page.



Warning - SMTP Configuration

E-mail Alert: Disable

SMTP Configuration

SMTP Server IP	192.168.0.1
Mail Account	user@192.168.0.1
□ Authentication	
User Name	
Password	
Confirm Password	
Rcpt E-mail Address 1	
Rcpt E-mail Address 2	
Rcpt E-mail Address 3	
Rcpt E-mail Address 4	

Field	Description
SMTP Server IP Address	Enter the IP address of the email Server
Authentication	Click on check box to enable password
User Name	Enter email Account name (Max.40 characters)
Password	Enter the password of the email account
Confirm Password	Re-type the password of the email account
You can set up to 4 email addresses to receive email alarm from Switch	
Rcpt E-mail Address 1	The first email address to receive email alert from Switch (Max. 40 characters)
Rcpt E-mail Address 2	The second email address to receive email alert from Switch (Max. 40 characters)
Rcpt E-mail Address 3	The third email address to receive email alert from Switch (Max. 40 characters)
Rcpt E-mail Address 4	The fourth email address to receive email alert from Switch (Max. 40 characters)

Once you finish configuring the settings, click on **Apply** to apply your configuration.

4.11.4 CLI Commands

Command Lines of the Warning configuration

Feature	Command Line
Event Selection	
Event Selection	Switch(config)# warning-event coldstart Switch cold start event warmstart Switch warm start event linkdown Switch link down event linkup Switch link up event authentication Authentication failure event super-ring Switch super ring topology change event time-sync Switch time synchronize event
Ex: Cold Start event	Switch(config)# warning-event coldstart Set cold start event enable ok.
Ex: Link Up event	Switch(config)# warning-event linkup [IFNAME] Interface name, ex: fastethernet1 or gi8 Switch(config)# warning-event linkup fa5

	Set fa5 link up event enable ok.
Display	Switch# show warning-event Warning Event: Cold Start: Enabled Warm Start: Disabled Authentication Failure: Disabled Link Down: fa4-5 Link Up: fa4-5 Super Ring Topology Change: Disabled Fault Relay: Disabled Time synchronize Failure: Disable
Syslog Configuration	
Local Mode	Switch(config)# log syslog local
Server Mode	Switch(config)# log syslog remote 192.168.2.200
Both	Switch(config)# log syslog local Switch(config)# log syslog remote 192.168.2.200
Disable	Switch(config)# no log syslog local
SMTP Configuration	
SMTP Enable	Switch(config)# smtp-server enable email-alert SMTP Email Alert set enable ok.
Sender mail	Switch(config)# smtp-server server 192.168.2.200 ACCOUNT SMTP server mail account, ex: support@westermo.se Switch(config)# smtp-server server 192.168.2.200 support@westermo.se SMTP Email Alert set Server: 192.168.2.200, Account: support@westermo.se ok.
Receiver mail	Switch(config)# smtp-server receipt 1 korecare@Westermo.com SMTP Email Alert set receipt 1: support@westermo.se ok.
Authentication with username and password	Switch(config)# smtp-server authentication username admin password admin SMTP Email Alert set authentication Username: admin, Password: admin ***Note: You can assign string to username and password.***

Disable SMTP	Switch(config)# no smtp-server enable email-alert SMTP Email Alert set disable ok.
Disable Authentication	Switch(config)# no smtp-server authentication SMTP Email Alert set Authentication disable ok.
Display	Switch# sh smtp-server SMTP Email Alert is Enabled Server: 192.168.2.20000, Account: admin@Westermo.com Authentication: Enabled Username: admin, Password: admin SMTP Email Alert Receipt: Receipt 1: support@westermo.se Receipt 2: Receipt 3: Receipt 4:

4.12 Monitor and Diag

The switch provides several types of features for you to monitor the status of the switch or diagnostic for you to check the problem when encountering problems related to the switch. The features include MAC Address Table, Port Statistics, Port Mirror, Event Log and Ping.
Following commands are included in this group:

4.12.1 MAC Address Table
4.12.2 Port Statistics
4.12.3 Port Mirror
4.12.4 Event Log
4.12.5 Topology Discovery (LLDP)
4.12.6 Ping
4.12.7 Modbus/TCP
4.12.8 CLI Commands of the Monitor and Diag

4.12.1 MAC Address Table

The switch provides 8K entries in MAC Address Table. In this page, users can change the Aging time, add Static Unicast MAC Address, monitor the MAC address or sort them by different packet types and ports. Click on **Apply** to change the value.

Aging Time (Sec)

Each switch fabric has limit size to write the learned MAC address. To save more entries for new MAC address, the switch fabric will age out non-used MAC address entry per Aging Time timeout. The default Aging Time is 300 seconds. The Aging Time can be modified in this page.

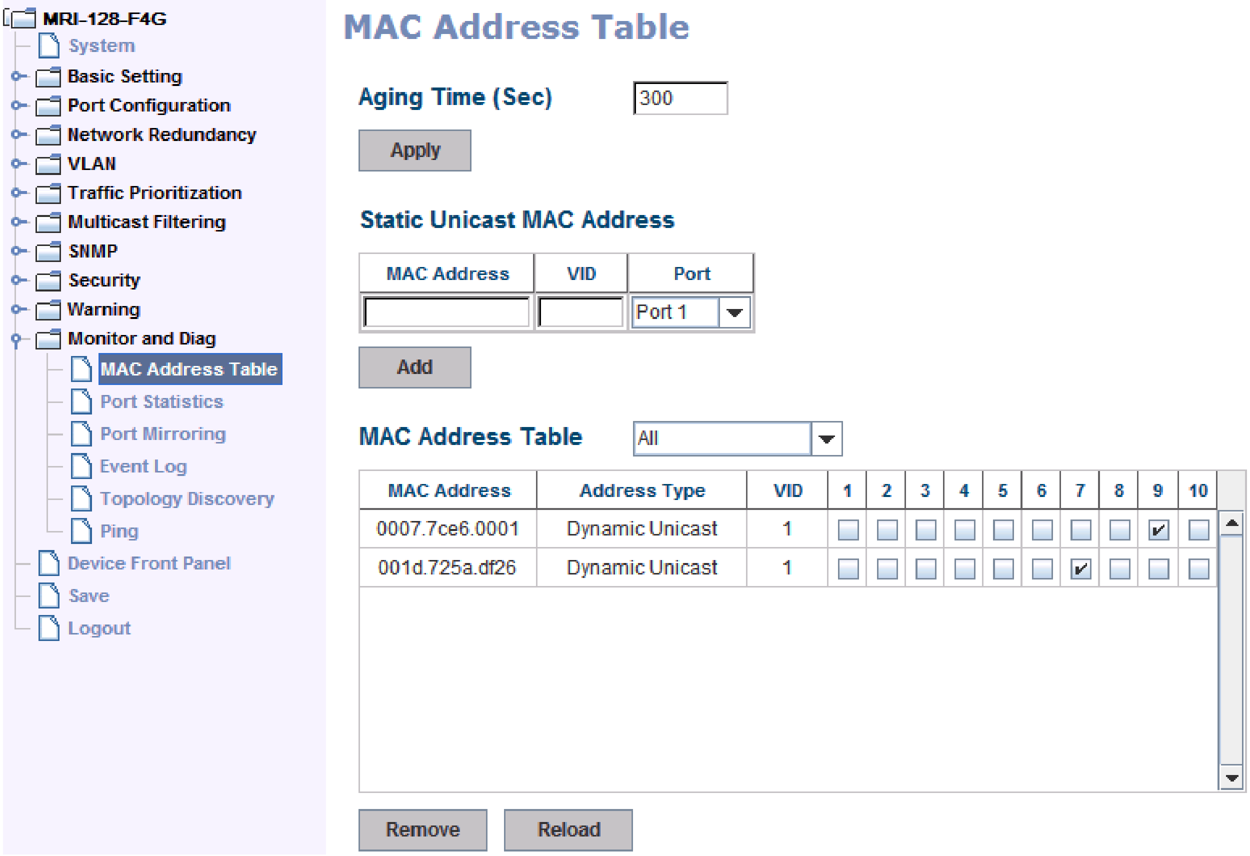
Static Unicast MAC Address

In some applications, users may need to type in the static Unicast MAC address to its MAC address table. In this page, you can type MAC Address (format: xxxx.xxxx.xxxx), select its VID and Port ID, and then click on **Add** to add it to MAC Address table.

MAC Address Table

In this MAC Address Table, you can see all the MAC Addresses learnt by the switch fabric. The packet types include Management Unicast, Static Unicast, Dynamic Unicast, Static Multicast and Dynamic Multicast. The table allows users to sort the address by the packet types and port.

Packet Types: Management Unicast means MAC address of the switch. It belongs to CPU port only. **Static Unicast** MAC address can be added and deleted. **Dynamic Unicast** MAC is MAC address learnt by the switch Fabric. **Static Multicast** can be added by CLI and can be deleted by Web and CLI. **Dynamic Multicast** will appear after you enabled IGMP and the switch learnt IGMP report. Click on **Remove** to remove the static Unicast/Multicast MAC address. Click on **Reload** to refresh the table. New learnt Unicast/Multicast MAC address will be updated to MAC address table.



MAC Address Table

Aging Time (Sec) 300

Apply

Static Unicast MAC Address

MAC Address	VID	Port
		Port 1

Add

MAC Address Table All

MAC Address	Address Type	VID	1	2	3	4	5	6	7	8	9	10
0007.7ce6.0001	Dynamic Unicast	1	□	□	□	□	□	□	□	□	☑	□
001d.725a.df26	Dynamic Unicast	1	□	□	□	□	□	□	☑	□	□	□

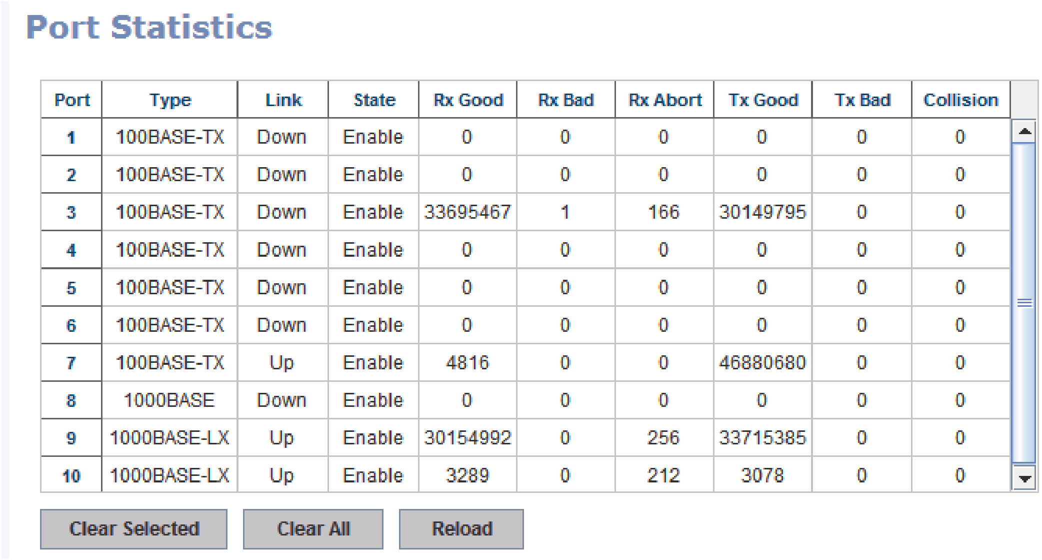
Remove Reload

4.12.2 Port Statistics

In this page, you can view operation statistics for each port. The statistics that can be viewed include Link Type, Link State, Rx Good, Rx Bad, Rx Abort, Tx Good, Tx Bad and Collision. Rx means the received packet while Tx means the transmitted packets.

Note: If you see many Bad, Abort or Collision counts increased, that may mean your network cable is not connected well, the network performance of the port is poor…etc. Please check your network cable, Network Interface Card of the connected device, the network application, or reallocate the network traffic…etc.

Click on **Clear Selected** to reinitialize the counts of the selected ports, and **Clear All** to reinitialize the counts of all ports. Click on **Reload** to refresh the counts.



Port Statistics

Port	Type	Link	State	Rx Good	Rx Bad	Rx Abort	Tx Good	Tx Bad	Collision
1	100BASE-TX	Down	Enable	0	0	0	0	0	0
2	100BASE-TX	Down	Enable	0	0	0	0	0	0
3	100BASE-TX	Down	Enable	33695467	1	166	30149795	0	0
4	100BASE-TX	Down	Enable	0	0	0	0	0	0
5	100BASE-TX	Down	Enable	0	0	0	0	0	0
6	100BASE-TX	Down	Enable	0	0	0	0	0	0
7	100BASE-TX	Up	Enable	4816	0	0	46880680	0	0
8	1000BASE	Down	Enable	0	0	0	0	0	0
9	1000BASE-LX	Up	Enable	30154992	0	256	33715385	0	0
10	1000BASE-LX	Up	Enable	3289	0	212	3078	0	0

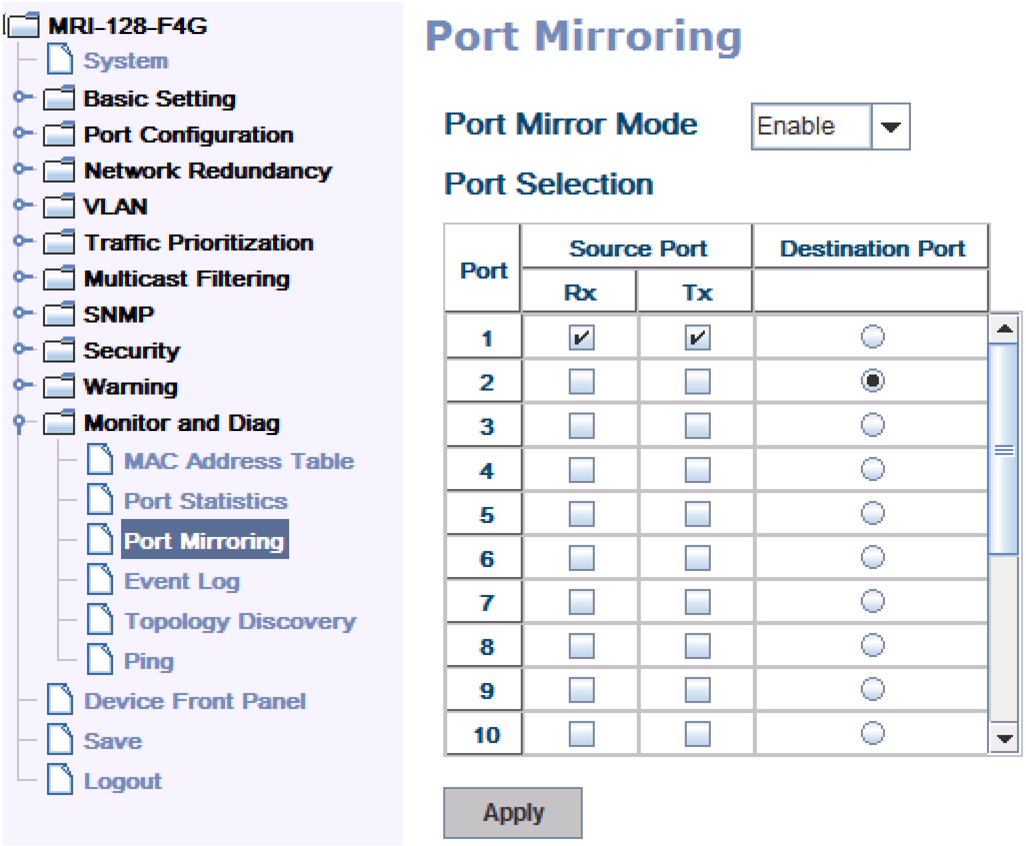
4.12.3 Port Mirroring

Port mirroring (also called port spanning) is a tool that allows you to mirror the traffic from one or more ports onto another port, without disrupting the flow of traffic on the original port. Any traffic that goes in or out of the Source Port(s) will be duplicated at the Destination Port. This traffic can then be analyzed on the Destination port using a monitoring device or application. A network administrator will typically utilize this tool for diagnostics, debugging, or fending off attacks.

Port Mirror Mode: Select Enable/Disable to enable/disable Port Mirror.

Source Port: This is also known as Monitor Port. These are the ports you want to monitor and the traffic of all source/monitor ports will be copied to destination/analysis ports. You can choose single port or any combination of ports, you can monitor them in Rx only, TX only or both RX and TX. Click on checkbox of the RX, Tx to select the source ports.

Destination Port: This is also known as Analysis Port. You can analyze the traffic of all the monitored ports at this port without affecting the flow of traffic on the port(s) being monitored. Only one of the destination ports can be selected. A network administrator would typically connect a LAN analyzer to this port.



Port Mirroring

Port Mirror Mode: Enable

Port Selection

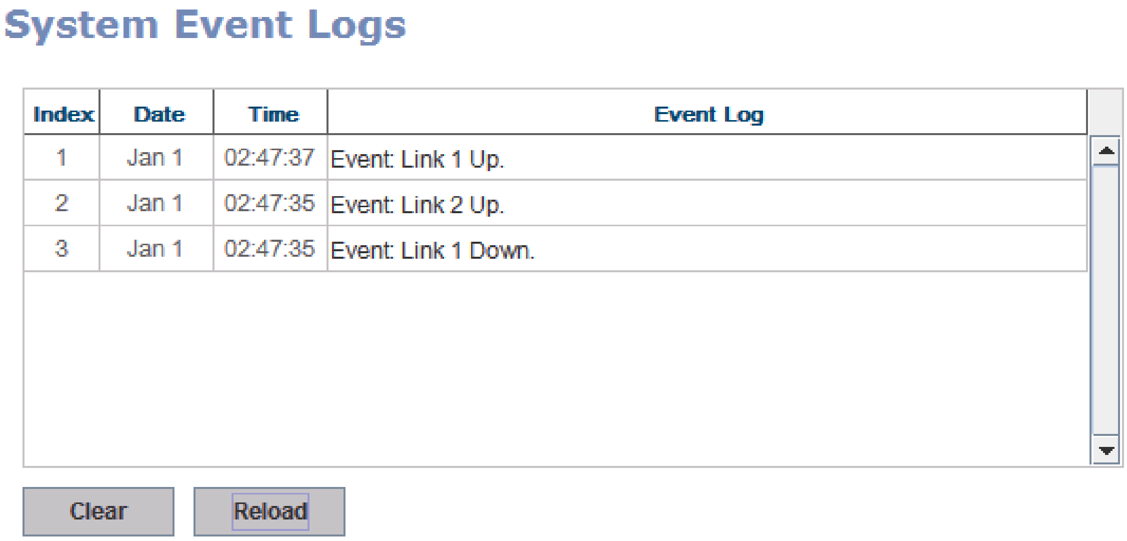
Port	Source Port		Destination Port
	Rx	Tx	
1	☑	☑	○
2	□	□	●
3	□	□	○
4	□	□	○
5	□	□	○
6	□	□	○
7	□	□	○
8	□	□	○
9	□	□	○
10	□	□	○

Once you finish configuring the settings, click on **Apply** to apply the settings.

4.12.4 Event Log

When System Log Local mode is selected, the switch will record occurred events in local log table. This page shows this log table. The entry includes the index, occurred data and time and content of the events.

Click on **Clear** to clear the entries. Click on **Reload** to refresh the table.

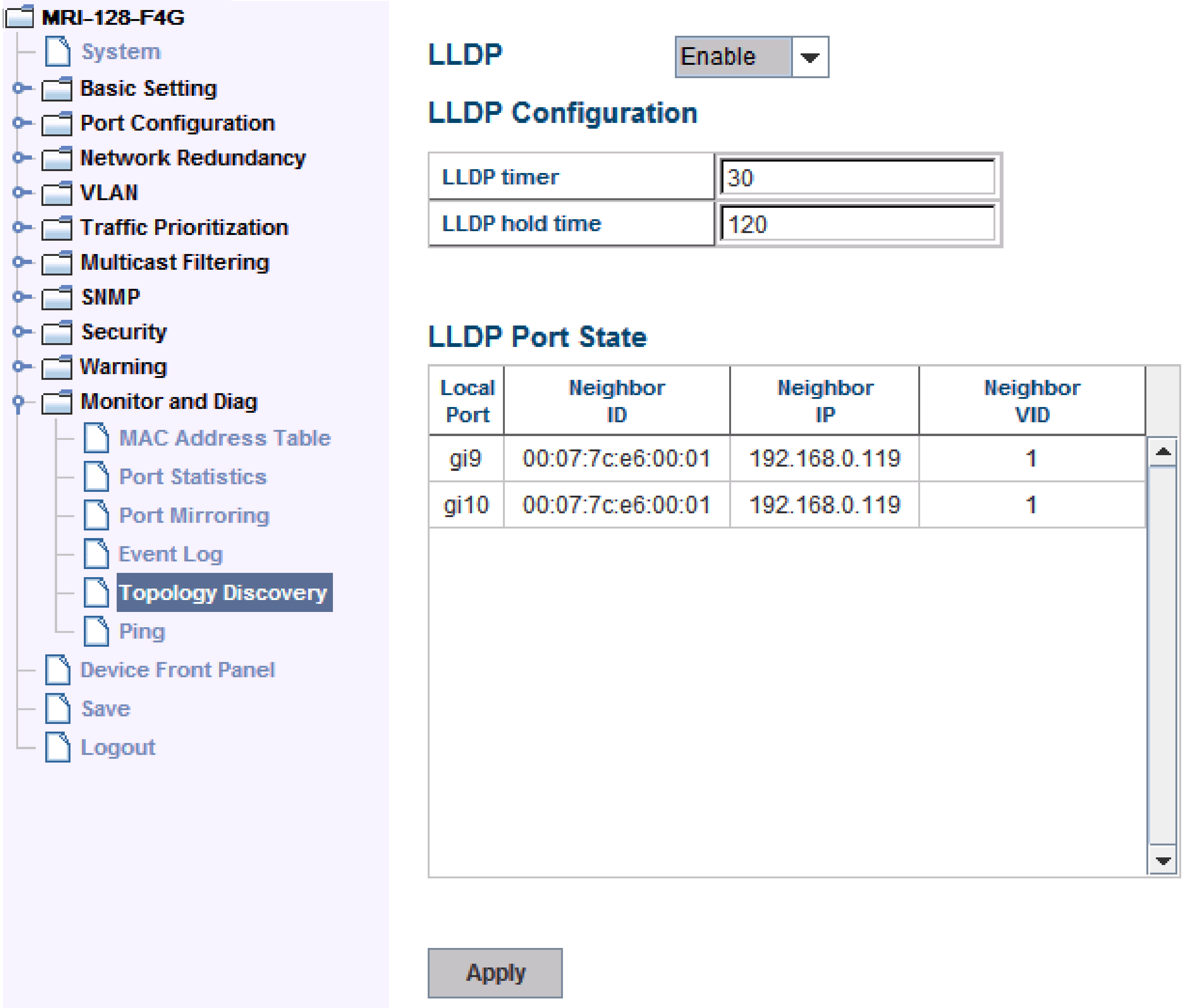


System Event Logs

Index	Date	Time	Event Log
1	Jan 1	02:47:37	Event: Link 1 Up.
2	Jan 1	02:47:35	Event: Link 2 Up.
3	Jan 1	02:47:35	Event: Link 1 Down.

4.12.5 Topology Discovery (LLDP)

The switch supports 802.1AB Link Layer Discovery Protocol, thus the switch can be discovered by the Network Management System which support LLDP discovery. With LLDP supported, the NMS can easier maintain the topology map, display port ID, port description, system description, VLAN ID… Once the link failure, the topology change events can be updated to the NMS as well. The LLDP Port State can display the neighbor ID and IP leant from the connected devices.



LLDP: Enable

LLDP Configuration

LLDP timer	30
LLDP hold time	120

LLDP Port State

Local Port	Neighbor ID	Neighbor IP	Neighbor VID
gi9	00:07:7c:e6:00:01	192.168.0.119	1
gi10	00:07:7c:e6:00:01	192.168.0.119	1

LLDP: Enable/Disable the LLDP topology discovery information.

LLDP Configuration: To configure the related timer of LLDP.

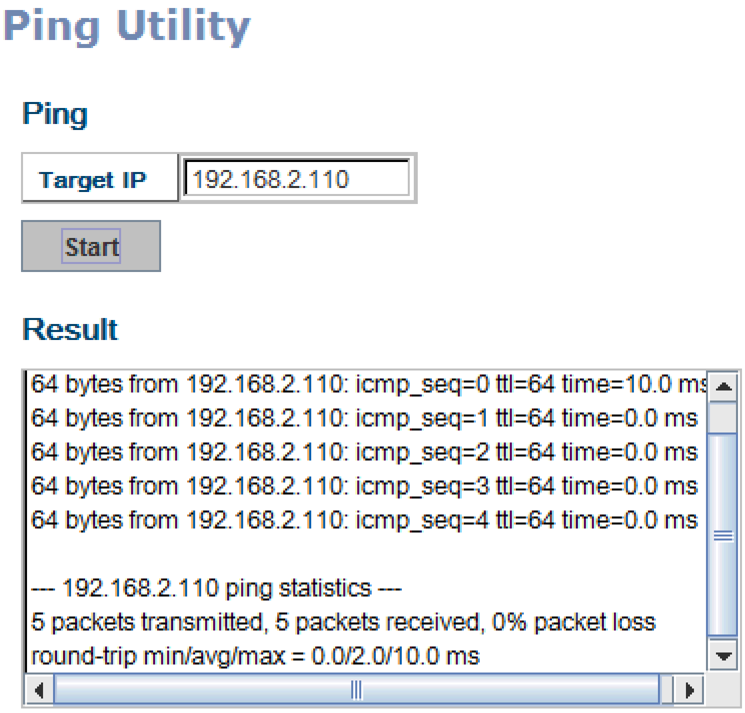
LLDP timer: The LLDPDP interval, the LLDP information is send per LLDP timer. The default value is 30 seconds.

LLDP hold time: The TTL (Time To Live) timer. The LLDP state will be expired once the LLDPDP is not received by the hold time. The default is 120 seconds.

LLDP Port State: Display the neighbor information learnt from the connected interface.

4.12.6 Ping Utility

This page provides **Ping Utility** for users to ping remote device and check whether the device is alive or not. Type **Target IP** address of the target device and click on **Start** to start the ping. After few seconds, you can see the result in the **Result** field.



Target IP: 192.168.2.110

```
64 bytes from 192.168.2.110: icmp_seq=0 ttl=64 time=10.0 ms
64 bytes from 192.168.2.110: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 192.168.2.110: icmp_seq=2 ttl=64 time=0.0 ms
64 bytes from 192.168.2.110: icmp_seq=3 ttl=64 time=0.0 ms
64 bytes from 192.168.2.110: icmp_seq=4 ttl=64 time=0.0 ms

--- 192.168.2.110 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/2.0/10.0 ms
```

4.12.7 Modbus/TCP

The Modbus is the most popular industrial protocol being used today. Modbus is a "master-slave" architecture, where the "master" sends polling request with address and data it wants to one of multiple "slaves". The slave device that is addressed responds to master. The master is often a PC, PLC, DCS or RTU… The salves are often the field devices. Some of them are "hybrid".

There are three most common Modbus versions, Modbus ASCII, Modbus RTU and Modbus/TCP. Ethernet based device, Industrial Ethernet Switch for example, supports Modbus/TCP that it can be polled through Ethernet. Thus the Modbus/TCP master can read or write the Modbus registers provided by the Industrial Ethernet Switch.

MRI-128-F4G implements the Modbus/TCP registers into the latest firmware. The registers include the System information, firmware information, IP address, interfaces' status, port information, SFP information, inbound/outbound packet information.

With the supported registers, users can read the information through their own

Modbus/TCP based progress/ display/ monitor applications and monitor the status of the switch easily.
There is no Web UI for Modbus/TCP configuration. The Modbus/TCP configuration can be changed through CLI.

Modbus/TCP Register Table

Word Address	Data Type	Description
System Information		
0x0000	16 words	Vender Name = “Westermo” Word 0 Hi byte = ‘W’ Word 0 Lo byte = ‘e’ Word 1 Hi byte = ‘s’ Word 1 Lo byte = ‘t’ Word 2 Hi byte = ‘e’ Word 2 Lo byte = ‘r’ Word 3 Hi byte = ‘m’ Word 3 Lo byte = ‘o’ Word 4 Hi byte = ‘\0’ (other words = 0)
0x0010	16 words	Product Name = "MRI-128-F4G" Word 0 Hi byte = ‘M’ Word 0 Lo byte = ‘R’ Word 1 Hi byte = ‘I’ Word 1 Lo byte = ‘-’ Word 2 Hi byte = ‘1’ Word 2 Lo byte = ‘2’ Word 3 Hi byte = ‘8’ Word 3 Lo byte = ‘-’ Word 4 Lo byte = ‘F’ Word 4 Hi byte = ‘4’ Word 5 Lo byte = ‘G’ Word 5 Hi byte = ‘\0’ (other words = 0)
0x0020	128 words	SNMP system name (string)
0x00A0	128 words	SNMP system location (string)
0x0120	128 words	SNMP system contact (string)

0x01A0	32 words	SNMP system OID (string)
0x01C0	2 words	System uptime (unsigned long)
0x01C2 to 0x01FF	60 words	Reserved address space
0x0200	2 words	hardware version
0x0202	2 words	S/N information
0x0204	2 words	CPLD version
0x0206	2 words	Boot loader version
0x0208	2 words	Firmware Version Word 0 Hi byte = major Word 0 Lo byte = minor Word 1 Hi byte = reserved Word 1 Lo byte = reserved
0x020A	2 words	Firmware Release Date Firmware was released on 2010-08-11 at 09 o’clock Word 0 = 0x0B09 Word 1 = 0x0A08
0x020C	3 words	Ethernet MAC Address Ex: MAC = 01-02-03-04-05-06 Word 0 Hi byte = 0x01 Word 0 Lo byte = 0x02 Word 1 Hi byte = 0x03 Word 1 Lo byte = 0x04 Word 2 Hi byte = 0x05 Word 2 Lo byte = 0x06
0x020F to 0x2FF	241 words	Reserved address space
0x0300	2 words	IP address Ex: IP = 192.168.10.1 Word 0 Hi byte = 0xC0 Word 0 Lo byte = 0xA8 Word 1 Hi byte = 0x0A Word 1 Lo byte = 0x01
0x0302	2 words	Subnet Mask
0x0304	2 words	Default Gateway
0x0306	2 words	DNS Server
0x0308 to	248 words	Reserved address space (IPv6 or others)

0x3FF		
0x0400	1 word	AC1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0401	1 word	AC2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0402	1 word	DC1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0403	1 word	DC2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0404 to 0x040F	12 words	Reserved address space
0x0410	1 word	DI1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0411	1 word	DI2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0412	1 word	DO1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0413	1 word	DO2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0414 to 0x041F	12 words	Reserved address space
0x0420	1 word	RDY

		0x0000:Off 0x0001:On
0x0421	1 word	RM 0x0000:Off 0x0001:On
0x0422	1 word	RF 0x0000:Off 0x0001:On
0x0423	1 word	RS
Port Information (32 Ports)		
0x1000 to 0x11FF	16 words	Port Description
0x1200 to 0x121F	1 word	Administrative Status 0x0000: disable 0x0001: enable
0x1220 to 0x123F	1 word	Operating Status 0x0000: disable 0x0001: enable 0xFFFF: unavailable
0x1240 to 0x125F	1 word	Duplex 0x0000: half 0x0001: full 0x0003: auto (half) 0x0004: auto (full) 0x0005: auto 0xFFFF: unavailable
0x1260 to 0x127F	1 word	Speed 0x0001: 10 0x0002: 100 0x0003: 1000 0x0004: 2500 0x0005: 10000 0x0101: auto 10 0x0102: auto 100 0x0103: auto 1000 0x0104: auto 2500 0x0105: auto 10000

		0x0100: auto 0xFFFF: unavailable
0x1280 to 0x129F	1 word	Flow Control 0x0000: off 0x0001: on 0xFFFF: unavailable
0x12A0 to 0x12BF	1 word	Default Port VLAN ID 0x0001-0xFFFF
0x12C0 to 0x12DF	1 word	Ingress Filtering 0x0000: disable 0x0001: enable
0x12E0 to 0x12FF	1 word	Acceptable Frame Type 0x0000: all 0x0001: tagged frame only
0x1300 to 0x131F	1 word	Port Security 0x0000: disable 0x0001: enable
0x1320 to 0x133F	1 word	Auto Negotiation 0x0000: disable 0x0001: enable 0xFFFF: unavailable
0x1340 to 0x135F	1 word	Loopback Mode 0x0000: none 0x0001: MAC 0x0002: PHY 0xFFFF: unavailable
0x1360 to 0x137F	1 word	STP Status 0x0000: disabled 0x0001: blocking 0x0002: listening 0x0003: learning 0x0004: forwarding
0x1380 to 0x139F	1 word	Default CoS Value for untagged packets
0x13A0 to 0x13BF	1 word	MDIX 0x0000: disable 0x0001: enable 0x0002: auto

		0xFFFF: unavailable
0x13C0 to 0x13DF	1 word	Medium mode 0x0000: copper 0x0001: fiber 0x0002: none 0xFFFF: unavailable
0x13E0 to 0x14FF	288 words	Reserved address space
SFP Information (32 Ports)		
0x1500 to 0x151F	1 word	SFP Type
0x1520 to 0x153F	1 words	Wave length
0x1540 to 0x157F	2 words	Distance
0x1580 to 0x167F	8 words	Vender
0x1680 to 0x17FF	384 words	Reserved address space
SFP DDM Information (32 Ports)		
0x1800 to 0x181F	1 words	Temperature
0x1820 to 0x185F	2 words	Alarm Temperature
0x1860 to 0x187F	1 words	Tx power
0x1880 to 0x18BF	2 words	Warning Tx power
0x18C0 to 0x18DF	1 words	Rx power
0x18E0 to 0x191F	2 words	Warning Rx power
0x1920 to 0x1FFF	1760 words	Reserved address space
Inbound packet information		
0x2000 to 0x203F	2 words	Good Octets
0x2040 to	2 words	Bad Octets

0x207F		
0x2080 to 0x20BF	2 words	Unicast
0x20C0 to 0x20FF	2 words	Broadcast
0x2100 to 0x213F	2 words	Multicast
0x2140 to 0x217F	2 words	Pause
0x2180 to 0x21BF	2 words	Undersize
0x21C0 to 0x21FF	2 words	Fragments
0x2200 to 0x223F	2 words	Oversize
0x2240 to 0x227F	2 words	Jabbers
0x2280 to 0x22BF	2 words	Discards
0x22C0 to 0x22FF	2 words	Filtered frames
0x2300 to 0x233F	2 words	RxError
0x2340 to 0x237F	2 words	FCSError
0x2380 to 0x23BF	2 words	Collisions
0x23C0 to 0x23FF	2 words	Dropped Frames
0x2400 to 0x243F	2 words	Last Activated SysUpTime
0x2440 to 0x24FF	191 words	Reserved address space
Outbound packet information		
0x2500 to 0x253F	2 words	Good Octets
0x2540 to 0x257F	2 words	Unicast

0x2580 to 0x25BF	2 words	Broadcast
0x25C0 to 0x25FF	2 words	Multicast
0x2600 to 0x263F	2 words	Pause
0x2640 to 0x267F	2 words	Deferred
0x2680 to 0x26BF	2 words	Collisions
0x26C0 to 0x26FF	2 words	SingleCollision
0x2700 to 0x273F	2 words	MultipleCollision
0x2740 to 0x277F	2 words	ExcessiveCollision
0x2780 to 0x27BF	2 words	LateCollision
0x27C0 to 0x27FF	2 words	Filtered
0x2800 to 0x283F	2 words	FCSError
0x2840 to 0x29FF	447 words	Reserved address space
Number of frames received and transmitted with a length(in octets)		
0x2A00 to 0x2A3F	2 words	64
0x2A40 to 0x2A7F	2 words	65 to 127
0x2A80 to 0x2ABF	2 words	128 to 255
0x2AC0 to 0x2AFF	2 words	256 to 511
0x2B00 to 0x2B3F	2 words	512 to 1023
0x2B40 to 0x2B7F	2 words	1024 to maximum size

4.12.8 CLI Commands of the Monitor and Diag

Command Lines of the Monitor and Diag configuration

Feature	Command Line
MAC Address Table	
Ageing Time	Switch(config)# mac-address-table aging-time 350 mac-address-table aging-time set ok! *Note: 350 is the new ageing timeout value.*
Add Static Unicast MAC address	Switch(config)# mac-address-table static 0007.7701.0101 vlan 1 interface fastethernet7 mac-address-table ucast static set ok! ***Note: rule: mac-address-table static MAC_address VLAN VID interface interface_name***
Add Multicast MAC address	Switch(config)# mac-address-table multicast 0100.5e01.0101 vlan 1 interface fa6-7 Adds an entry in the multicast table ok! ***Note: rule: mac-address-table multicast MAC_address VLAN VID interface_list interface_name/range***
Show MAC Address Table – All types	Switch# show mac-address-table ***** UNICAST MAC ADDRESS ***** Destination Address Address Type Vlan Destination Port ------------------- --------------- ------- ------------------------ 000f.b079.ca3b Dynamic 1 fa4 0007.7c01.0386 Dynamic 1 fa7 0007.7c10.0101 Static 1 fa7 0007.7c10.0102 Static 1 fa7 0007.7cff.0100 Management 1 ***** MULTICAST MAC ADDRESS *****

	Vlan Mac Address COS Status Ports ---- --------------- ---- ------- -------------------------- 1 0100.5e40.0800 0 fa6 1 0100.5e7f.fffa 0 fa4,fa6
Show MAC Address Table – Dynamic Learnt MAC addresses	Switch# show mac-address-table dynamic Destination Address Address Type Vlan Destination Port ------------------- --------------- ------- ------------------------ 000f.b079.ca3b Dynamic 1 fa4 0007.7c01.0386Dynamic 1 fa7
Show MAC Address Table – Multicast MAC addresses	Switch# show mac-address-table multicast Vlan Mac Address COS Status Ports ---- --------------- ---- ------- -------------------------- 1 0100.5e40.0800 0 fa6-7 1 0100.5e7f.fffa 0 fa4,fa6-7
Show MAC Address Table – Static MAC addresses	Switch# show mac-address-table static Destination Address Address Type Vlan Destination Port ------------------- --------------- ------- ------------------------ 0007.7c10.0101 Static 1 fa7 0007.7c10.0102 Static 1 fa7
Show Aging timeout time	Switch# show mac-address-table aging-time the mac-address-table aging-time is 300 sec.
Port Statistics	
Port Statistics	Switch# show rmon statistics fa4 (select interface) Interface fastethernet4 is enable connected, which has Inbound: Good Octets: 178792, Bad Octets: 0 Unicast: 598, Broadcast: 1764, Multicast: 160 Pause: 0, Undersize: 0, Fragments: 0 Oversize: 0, Jabbers: 0, Disacrds: 0 Filtered: 0, RxError: 0, FCSError: 0 Outbound: Good Octets: 330500 Unicast: 602, Broadcast: 1, Multicast: 2261

	Pause: 0, Deferred: 0, Collisions: 0 SingleCollision: 0, MultipleCollision: 0 ExcessiveCollision: 0, LateCollision: 0 Filtered: 0, FCSError: 0 Number of frames received and transmitted with a length of: 64: 2388, 65to127: 142, 128to255: 11 256to511: 64, 512to1023: 10, 1024toMaxSize: 42
Port Mirroring	
Enable Port Mirror	Switch(config)# mirror en Mirror set enable ok.
Disable Port Mirror	Switch(config)# mirror disable Mirror set disable ok.
Select Source Port	Switch(config)# mirror source fa1-2 both Received and transmitted traffic rx Received traffic tx Transmitted traffic Switch(config)# mirror source fa1-2 both Mirror source fa1-2 both set ok. ***Note: Select source port list and TX/RX/Both mode.***
Select Destination Port	Switch(config)# mirror destination fa6 both Mirror destination fa6 both set ok
Display	Switch# show mirror Mirror Status : Enabled Ingress Monitor Destination Port: fa6 Egress Monitor Destination Port: fa6 Ingress Source Ports :fa1,fa2, Egress Source Ports :fa1,fa2,
Event Log	
Display	Switch# show event-log <1>Jan 1 02:50:47 snmpd[101]: Event: Link 4 Down. <2>Jan 1 02:50:50 snmpd[101]: Event: Link 5 Up. <3>Jan 1 02:50:51 snmpd[101]: Event: Link 5 Down. <4>Jan 1 02:50:53 snmpd[101]: Event: Link 4 Up.
Topology Discovery (LLDP)	
Enable LLDP	Switch(config)# lldp holdtime Specify the holdtime of LLDP in seconds

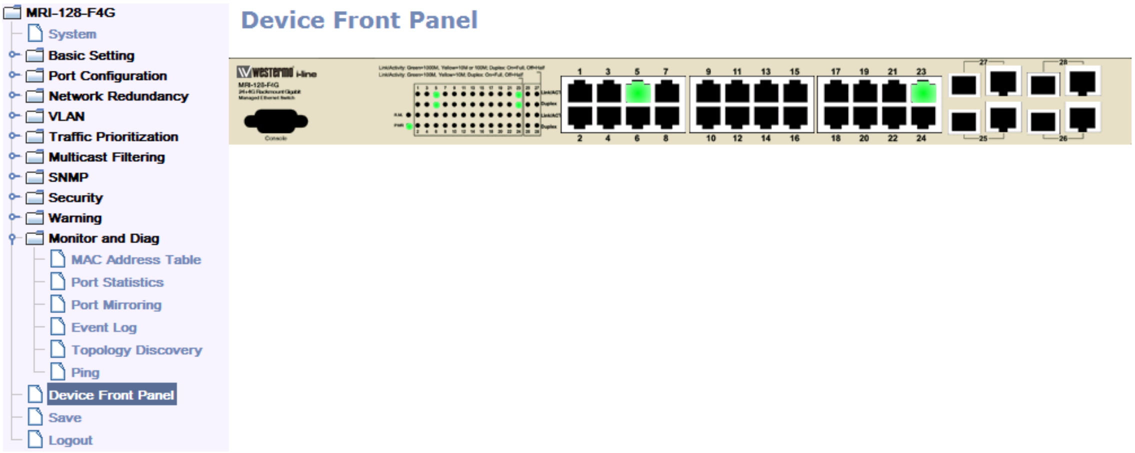
	run Enable LLDP timer Set the transmission frequency of LLDP in seconds Switch(config)# lldp run LLDP is enabled!
Change LLDP timer	Switch(config)# lldp holdtime <10-255> Valid range is 10~255 Switch(config)# lldp timer <5-254> Valid range is 5~254
Ping	
Ping IP	Switch# ping 192.168.2.33 PING 192.168.2.33 (192.168.2.33): 56 data bytes 64 bytes from 192.168.2.33: icmp_seq=0 ttl=128 time=0.0 ms 64 bytes from 192.168.2.33: icmp_seq=1 ttl=128 time=0.0 ms 64 bytes from 192.168.2.33: icmp_seq=2 ttl=128 time=0.0 ms 64 bytes from 192.168.2.33: icmp_seq=3 ttl=128 time=0.0 ms 64 bytes from 192.168.2.33: icmp_seq=4 ttl=128 time=0.0 ms --- 192.168.2.33 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms
Modbus/TCP	
Number of the Modbus/TCP Master	Switch(config)# modbus idle-timeout Max interval between requests master Modbus TCP Master port Listening Port Switch(config)# modbus master <1-20> Max Modbus TCP Master
Modbus/TCP idle time	Switch(config)# modbus idle-timeout <200-10000> Timeout vlaue: 200-10000ms
Modbus/TCP port number	Switch(config)# modbus port <1-65535> Port Number

4.12 Device Front Panel

Device Front Panel allows you to see LED status on the switch. You can see LED and link status of the Power, DO, DI, R.M. and Ports.

Feature	On / Link UP	Off / Link Down	Note
Power	Green	Black	
R.M. (Ring Master)	Green	Black	
Port Link LED	Green	Black	
Port Active LED	Green	Black	
Port Link State	Green	Black	Green: The port is connected. Black: Not connected.
SFP Link State	Green	Black	Gray: Plugged but not link up yet.

The switch Front Panel



Note: No CLI command for this feature.

4.13 Save to Flash

Save Configuration allows you to save any configuration you just made to the Flash. Powering off the switch without clicking on **Save Configuration** will cause loss of the new settings. After selecting **Save Configuration**, click on **Save to Flash** to save your new configuration.

Command Lines:

Feature	Command Line
Save	SWITCH# write Building Configuration… [OK] Switch# copy running-config startup-config Building Configuration... [OK]

4.14 Logout

The switch provides two logout methods. The web connection will be logged out if you don’t input any command after 30 seconds. The Logout command allows you to manually logout the web connection. Click on **Yes** to logout, **No** to go back the configuration page.

Command Lines:

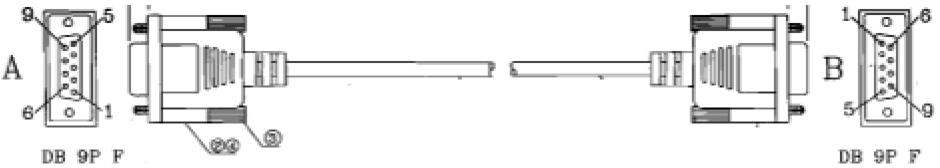
Feature	Command Line
Logout	SWITCH> exit SWITCH# exit

5 Appendix

5.1 Pin Assignment of the RS-232 Console Cable

The total cable length is 150cm.

A	B
1	1
2	3
3	2
4	6
5	5
6	4
7	8
8	7
9	9



5.2 Private MIB

The private MIB can be found in product CD. Compile the private MIB file by your SNMP tool. The private MIB tree is the same as the web tree. This is easier to understand and use. If you are not familiar with standard MIB, you can directly use private MIB to manage/monitor the switch, no need to learn or find where the OIDs of the commands are.

5.3 Revision History

Edition	Date	Modifications
V1.2	2014/9/29	• 4.11.4 CLI commands updated • 4.12.7 Modbus/TCP updated
V1.1	2013/11/1	• Add IPv6, Multiple Spanning Tree Protocol, Private VLAN, QinQ, GMRP and Modbus/TCP features • Update daylight saving time picture • Update the combo port behavior. • Update IGMP Unknown Multicast description. • Update MSR description and Network Redundancy commands.
V1.0	2010/11/9	The first release

Westermo • SE-640 40 Stora Sundby, Sweden
Tel +46 16 42 80 00 Fax +46 16 42 80 01
E-mail: info@westermo.com
www.westermo.com

Sales Units
Westermo Data Communications

China
sales.cn@westermo.com
www.cn.westermo.com

France
infos@westermo.fr
www.westermo.fr

Germany
info@westermo.de
www.westermo.de

North America
info@westermo.com
www.westermo.com

Singapore
sales@westermo.com.sg
www.westermo.com

Sweden
info.sverige@westermo.se
www.westermo.se

United Kingdom
sales@westermo.co.uk
www.westermo.co.uk

Other Offices

For complete contact information, please visit our website at www.westermo.com/contact or scan the QR code with your mobile phone.