MDI-110 Series

User's Manual

Version 1.1

Industrial Managed Ethernet Switch

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 Westermo i-line MDI-110 Series User Manual. Following topics are covered in this chapter:

1.1 Overview

1.2 Major Features

1.3 Package Checklist

1.1 Overview

MDI-110 series, Industrial 10-port Managed Ethernet Switches, have 7 10/100Base-TX ports and 3 combo ports, 10/100/1000 RJ-45 / 100-FX / Gigabit SX/LX for MDI-110-F3G and 10/100 RJ-45 / 100-FX SX/LX for MDI-110-F3. MDI-110 is especially designed to operate under harsh environmental conditions. The switches provide solid foundation for a highly fault-tolerant and easily-managed network. MDI-110 can be remotely configured by Telnet, Web browser, WeDashboard and managed by Simple Network Management Protocol (SNMP) and Remote Monitoring (RMON). You can also connect the attached RS232 console cable to manage the switch via a Command Line Interface (CLI). CLI commands are Cisco-like commands, your engineers who are familiar with Cisco products don’t need to learn new rules for CLI commands.

Security is enhanced with advanced features such as 802.1Q VLAN and Port/IP security. Performance is optimized by QoS and IGMP Snooping/Query. Westermo ring technology, Multiple Super Ring, enables superb self-healing capability for network failure. This is Westermo patented ring technology, which is registered in most countries. For interoperability with your existed network, MDI-110 series also come with an advanced redundant network solution, Ring Coupling and Rapid Dual Homing technology. With Ring Coupling and Rapid Dual Homing technology, Ethernet Ring can be extended more easily. No matter which Westermo switch or other managed switches.

The IP31-designed aluminum case further strengthens MDI-110's withstand ability in harsh industrial environment. The event warning is notified to the network administrator via e-mail, system log, or to field engineers by relay output. MDI-110 Series Industrial Managed Ethernet Switch has also passed CE/ FCC/ UL safety certifications to help ensure safe and reliable data transmission for industrial applications

1.2 Major Features

The products have the following features:

- MDI-110-F3G: 7 10/100 Base TX and 3 Gigabit RJ-45/SFP combo (10/100/1000 Base-TX, 100 FX, Gigabit SX/LX)
- MDI-110-F3: 7 10/100 Base TX and 3 100Mbps RJ-45/SFP combo (10/100 Base-TX, 100 FX SX/LX)
- Multiple Super Ring (recovery time <5ms), Rapid Dual Homing, Multiple Ring, and MSTP/RSTP
- VLAN, Private VLAN, QinQ, GVRP, QoS, IGMP Snooping V1/V2/V3, Rate Control, Port Trunking, LACP, Online Multi-Port Mirroring
- 32Gbps Non-Blocking, switch backplane 8K MAC address table
- Supports console CLI , Web, LLDP, SNMP V1/V2c/V3, RMON, HTTPS, SSH, and WeDashboard for remote management
- Embedded Hardware Watchdog timer to auto reset when failure
- Advanced security feature supports IP Security, Port Security, advanced SSHL/SSL authentication key configuration, Telnet/Http service control
- DHCP Server with advanced function –DHCP option 82 with Relay circuit, DHCP server by port based, IP and MAC Binding, 802.1x network access control.
- Event Notification by E-mail, SNMP trap, Syslog, Digital Input and Relay Output
- Supports Modbus TCP/IP client for Factory Automation
- Supports Multiple Language for Web User Interface
- Industrial Heat dispersing design, -25~70˚C operating temperature, Rigid Aluminum Case Complies with IP31 –For more wide operating temperature, please contact your sales window.

Note: The detail spec is listed in Appendix 5.1.

1.3 Package List

The products are shipped with following items:

- One Industrial Managed Ethernet Switch
- One DIN-Rail clip (attached to the switch)
- One wall mounting plate and 4 screws (M3, 6 mm long)
- One RS-232 DB-9 to RJ-45 console cable
- Documentation and Software CD
- Quick Installation Guide

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

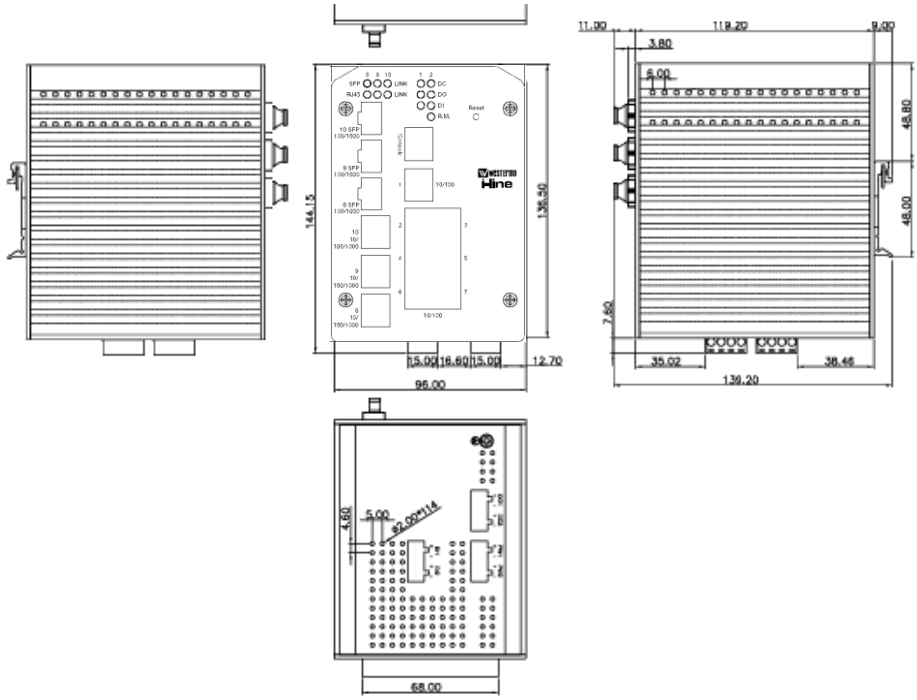
2 Hardware Installation

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

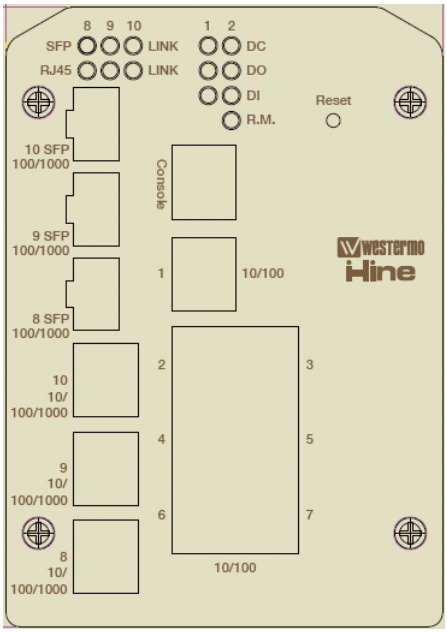
2.1 Hardware Introduction

Dimension

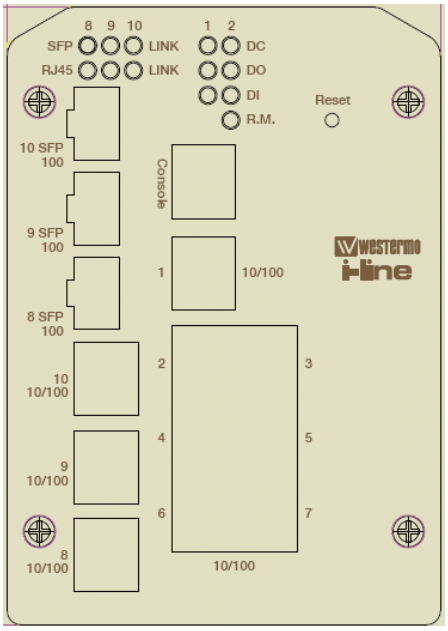
The switch dimension (W x H x D) is **96mm x 137mm x 119mm**



Panel Layout



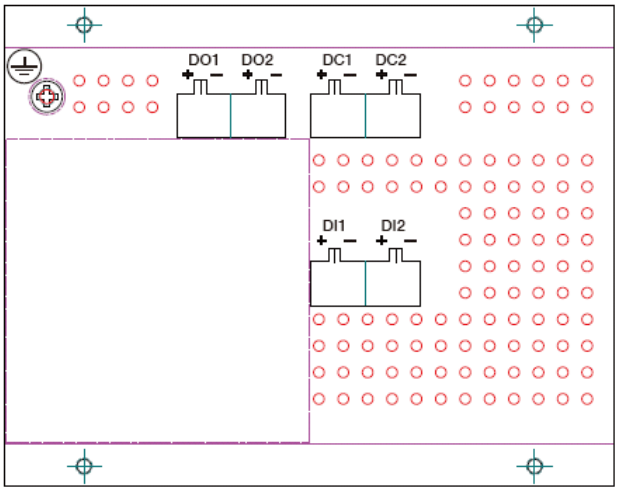
MDI-110-F3G



MDI-110-F3

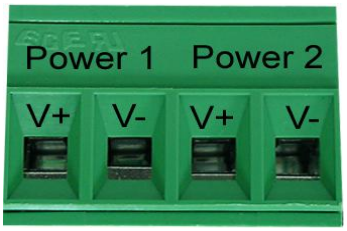
Bottom View

The bottom view of the switch consists of three terminal block connectors with two DC power inputs, two Digital Inputs, two Relay Outputs and one Earth Ground.

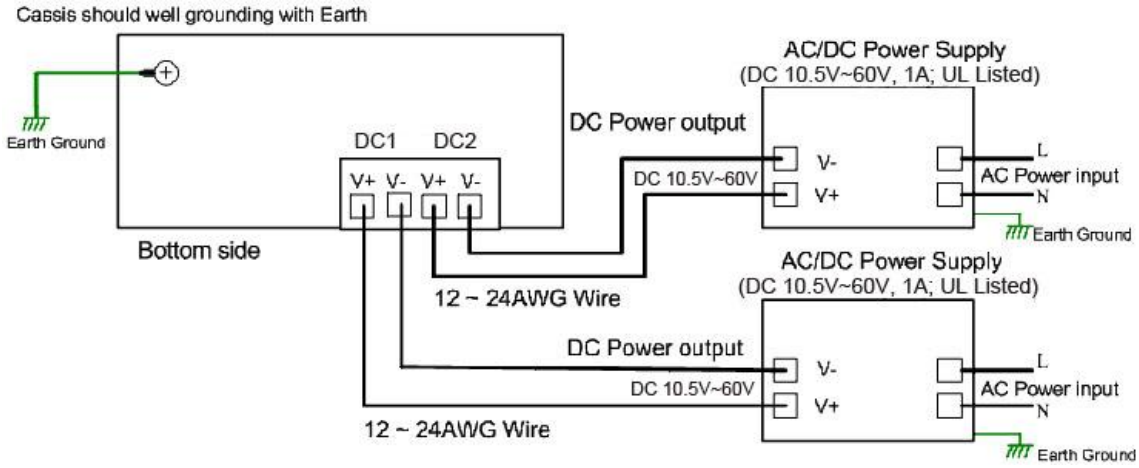


2.2 Wiring Power Inputs

Follow below steps to wire the redundant DC power inputs.



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 and polarity reverse protection functions.
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 electric wire is from 12 to 24 AWG.

Note 3: If the 2 power inputs are connected, the switch will be powered from the highest connected voltage. The unit will alarm for loss of power, either POWER1 or POWER2.

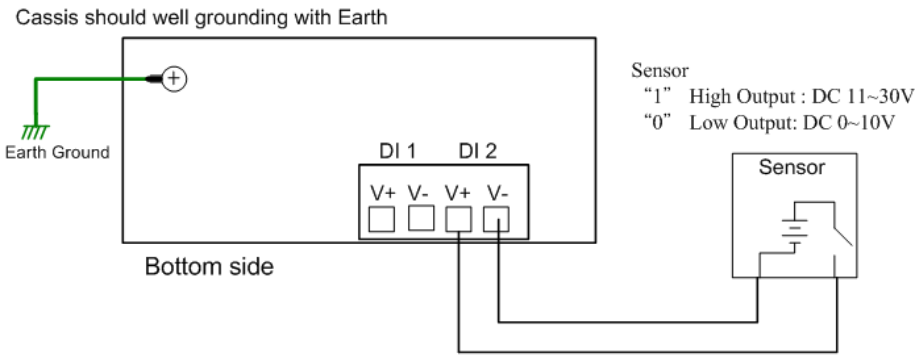
Note 4: Use a UL Listed Power supply with output Rating 10.5-60VDC, minimum 1 A.

2.3 Wiring Digital Input

The switch provides 2 digital inputs. It allows users to connect the termination units' digital output and manage/monitor the status of the connected unit. The Digital Input pin can be pulled high or low; thus the connected equipment can actively drive these pins high or low. The embedded software UI allows you to read and set the value to the connected device.

The power input voltage of logic low is DC 0~10V. Logic high is DC 11~30V.

Wire the digital input just like wiring the power input introduced in chapter 2.2.

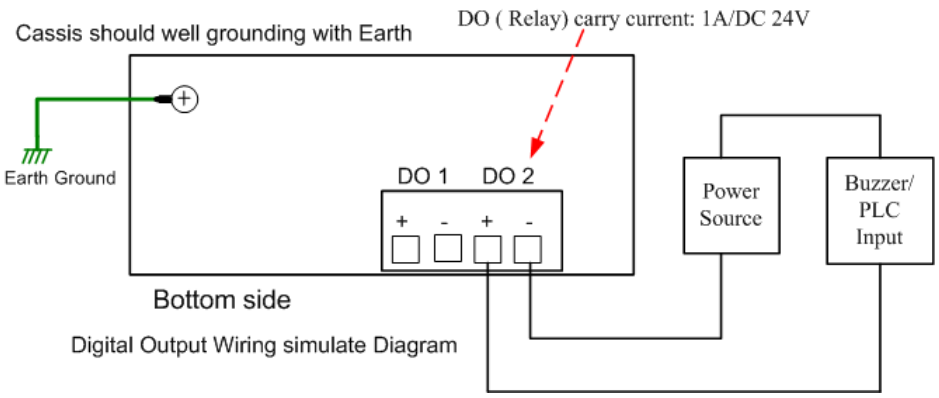


Digital Input Wiring simulate Diagram

2.4 Wiring Digital Output

The switch provides 2 digital outputs, also known as Relay Output. The relay contacts are energized (open) for normal operation and will close for fault conditions. The fault conditions include power failure, Ethernet port link break or other pre-defined events which can be configured in the switch UI.

Wiring digital output is exactly the same as wiring power input introduced in chapter 2.2.



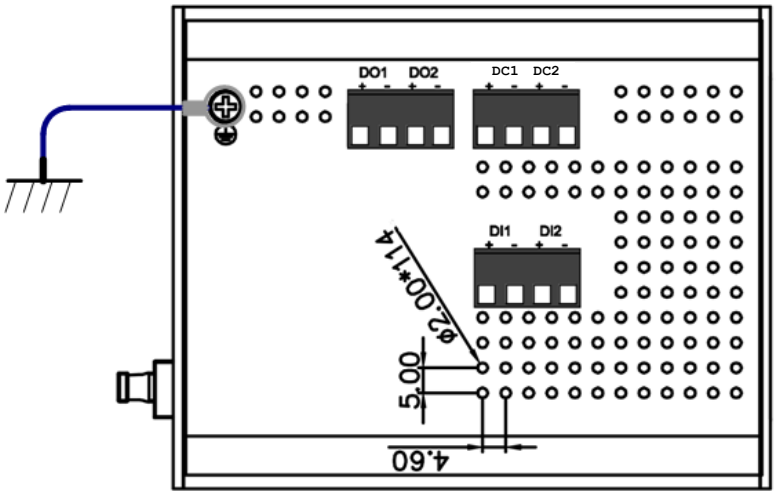
Digital Output Wiring simulate Diagram

2.5 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 the Earth Ground.

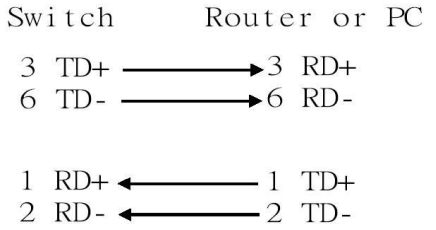
On the bottom side of the switch, there is one earth ground screw. Loosen the earth ground screw using a screw-driver; then tighten the screw after earth ground wire is connected.



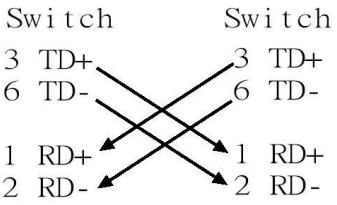
2.6 Wiring Fast Ethernet Ports

The switch includes 7 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)

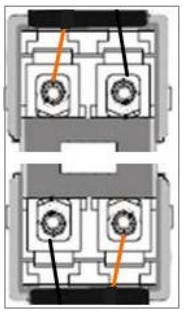
1000 Base-TX: 4-pair UTP/STP Cat. 5 cable, EIA/TIA-568 100-ohm (100m)

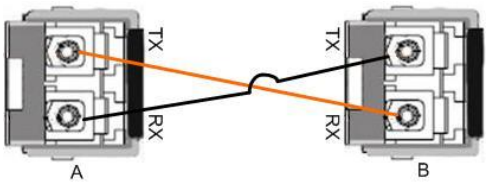
2.7 Wiring Fiber Ports

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 fist. 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 stare at the Laser/LED Beam.

2.8 Wiring Combo Ports

The switch includes 3 RJ-45/SFP combo ports. The SFP ports accept standard MINI GBIC SFP transceiver. To ensure system reliability, it is strongly recommended to use the Westermo i-line certificated SFP Transceiver. The certificated SFP transceiver includes 100Base-FX single/multi mode, 1000Base-SX/LX single/multi mode with ranges from 550m to 80km.

Note: The Ethernet Switch has to use UL recognized fiber transceiver with Class

1 Laser/LED Diode.

Note: It is recommended not to plug in SFP fiber transceiver and link up RJ-45 port at same time, it might cause the connection does not work properly.

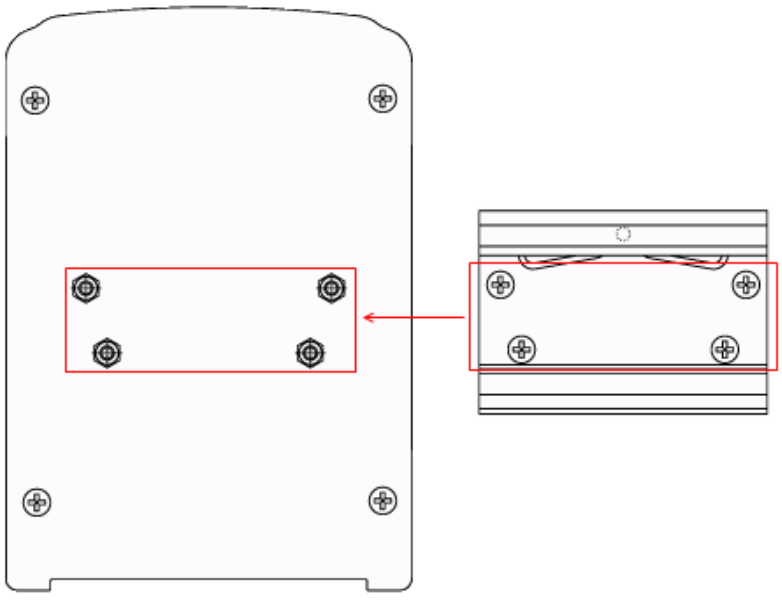
2.9 Wiring RS-232 Console Cable

Westermo attaches one RS-232 DB-9 to RJ-45 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 have lost the cable, please contact your sales office or follow the pin assignment to buy/make a new one. The pin assignment spec is listed in the appendix.

2.10 DIN-Rail Mounting Installation

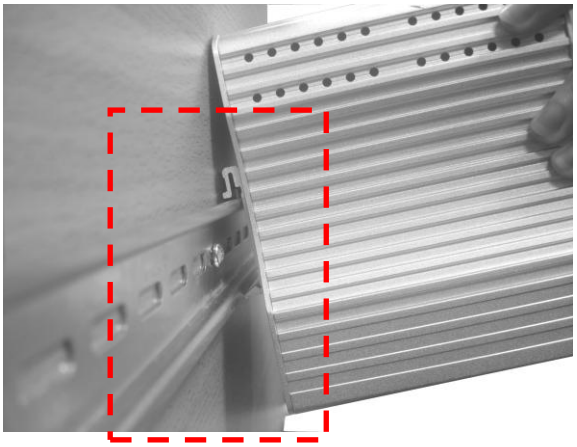
The DIN-Rail clip is already attached to the switch when packaged. If the DIN-Rail clip is not screwed on the switch, follow the instructions and the figure below to attach the DIN-Rail clip to the switch.



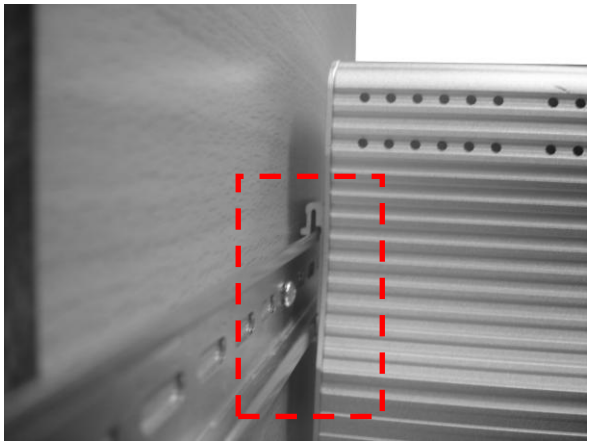
1. Use the screws to attach DIN-Rail clip to the rear panel.
2. To remove DIN-Rail clip, reverse step 1.

Follow the steps below to mount the switch on a DIN-Rail track:

1. First, insert the upper end of the DIN-Rail clip into the back of the DIN-Rail track from its upper side.



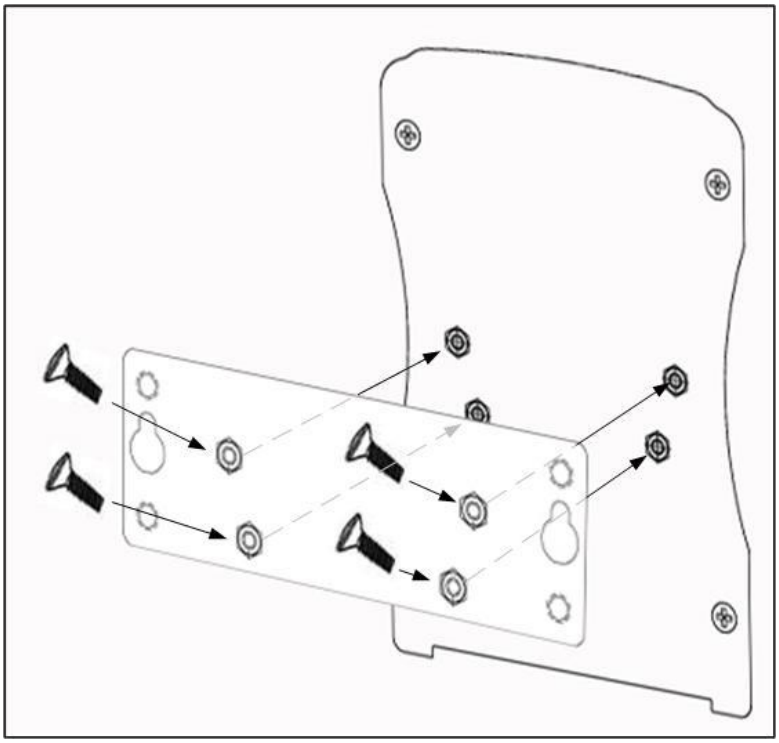
2. Lightly push the bottom of DIN-Rail clip into the track.



3. Check if the DIN-Rail clip is tightly attached to the track.
4. To remove the switch from the track, reverse the steps above.

Note: The DIN-Rail track should comply with DIN EN50022 standard. Using the wrong DIN-Rail track may cause an unsafe system install.

2.11 Wall-Mounting Installation



Follow the steps below to install the switch with the wall mounting plate.

1. To remove the DIN-Rail clip from the switch, loosen the screws.
2. Place the wall mounting plate on the rear panel of the switch.
3. Use the screws to tighten the wall mounting plate onto the switch.
4. Use the hook holes at the corners of the wall mounting plate to hang the switch onto the wall.
5. To remove the wall mounting plate, reverse the steps above.

Note: To avoid damage the internal circuit, be sure use the screw included in the package to screw the wall-mount kit onto the rear side of the switch. The specification of the screws is M3, 6 mm long.

2.12 Safety Warning

The Equipment intended for installation in a Restricted Access Location.

Restricted Access Location:

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

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 RS-232 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, SSH 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

Note: It is recommended management session don't exceed 2 accounts for Web and Telnet management. Once the session exceeds 3 accounts, the system kernel may show some information in the local / telnet interface.

3.1 Preparation for Serial Console

In the package, Westermo attached one RS-232 DB-9 to RJ-45 console cable. Please attach RS-232 DB-9 connector to your PC COM port, connect RJ-45 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 local 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 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 2.3-20101014-11:04:13).

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

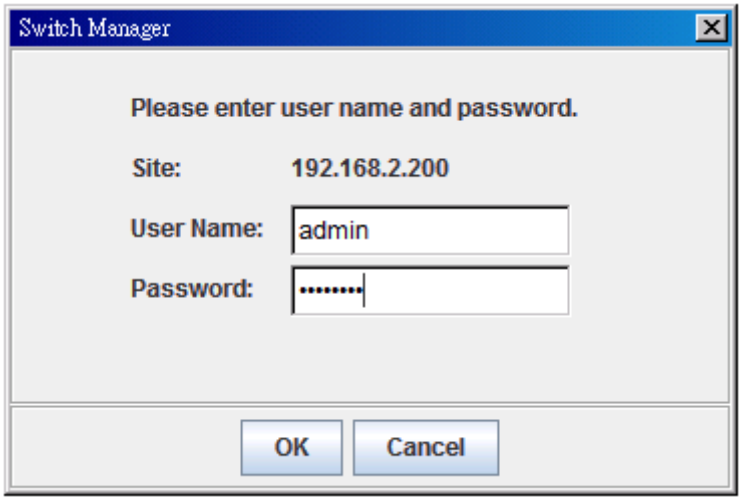
Westermo web management page is developed by JAVA. It allows you to use a standard web-browser such as Microsoft Internet Explorer, or Mozilla Firefox, to configure and/or log from the switch from anywhere on the network.

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

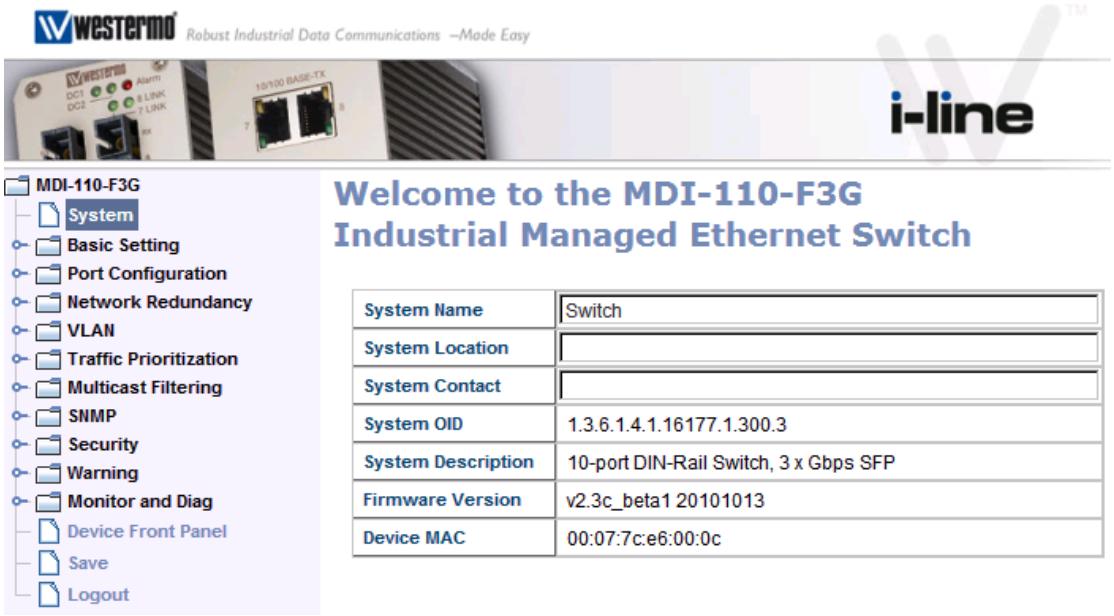
1. Verify that your network interface card (NIC) is operational, and that your operating system supports TCP/IP protocol.
2. Wire DC power to the switch and connect your switch to your computer.
3. Make sure that the switch default IP address is 192.168.2.200.
4. Change your computer IP address to 192.168.2.2 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**.



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



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

Note 1: Internet Explorer (IE) 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.

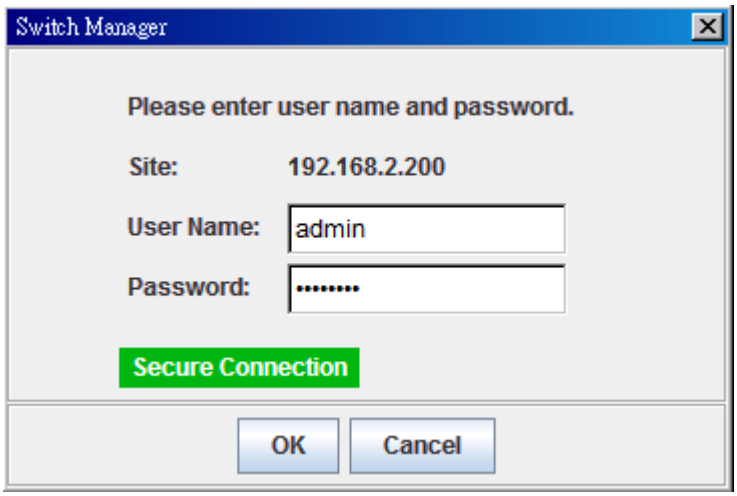
Note 2: The Web UI connection session will be logged out automatically if you don't give any input after 30 seconds. After logged out, you should re-login and type in the correct user name and password again.

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 log in.

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.



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 a 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.

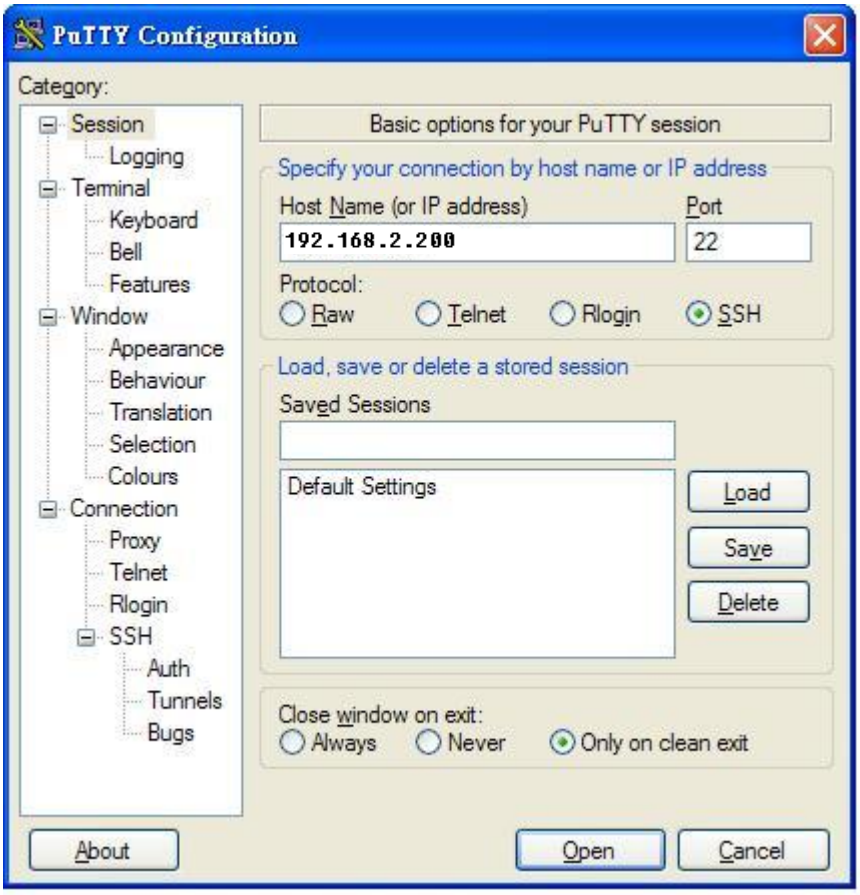
When you wish to establish a SSH connection with the switch, you should download the SSH client tool first.

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 by SSH. Note: PuTTY is copyright 1997-2006 Simon Tatham.

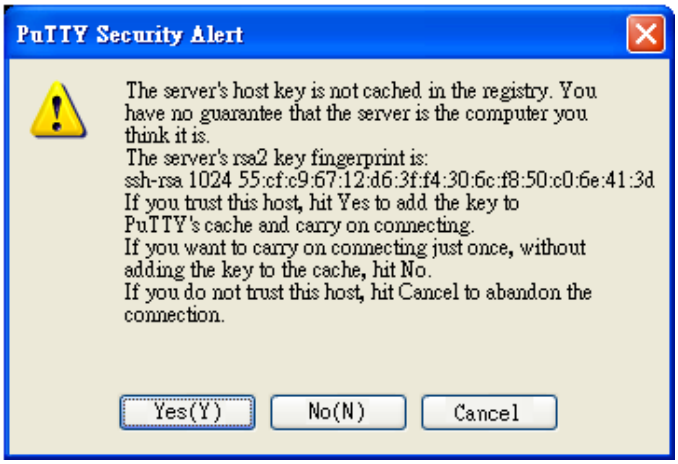
1. Open SSH Client/PuTTY

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



"**Open**" to start the SSH session console.

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



3. After few seconds, the SSH connection to the switch is opened.
4. Type the Login Name and its Password. The default Login Name and Password are **admin/westermo**.

5. 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 software features. There are four ways to access the switch: Serial console, Telnet/SSH, Web browser and SNMP.

The Industrial Managed 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 the network connection to your Switch. This is so-called out-band management. It wouldn't be affected by the network performance.

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. Then you can remotely connect to its embedded HTML web pages or Telnet console.

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

Note: IE 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.

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 and 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. **?** 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. **?** to see the command

```
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. **?** 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 for you to see these available commands. Save your time in typing and avoid typing error.

? 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
```

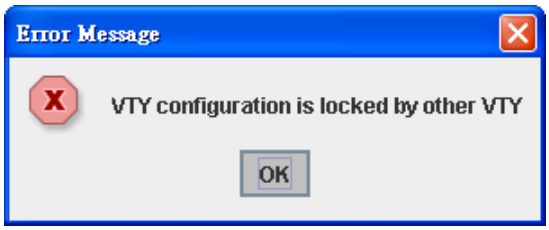
Tab This tab key helps you to input the command quicker. If there is only one available command in the next, clicking on tab key can help to finish typing soon.

```
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.



4.2 Basic Setting

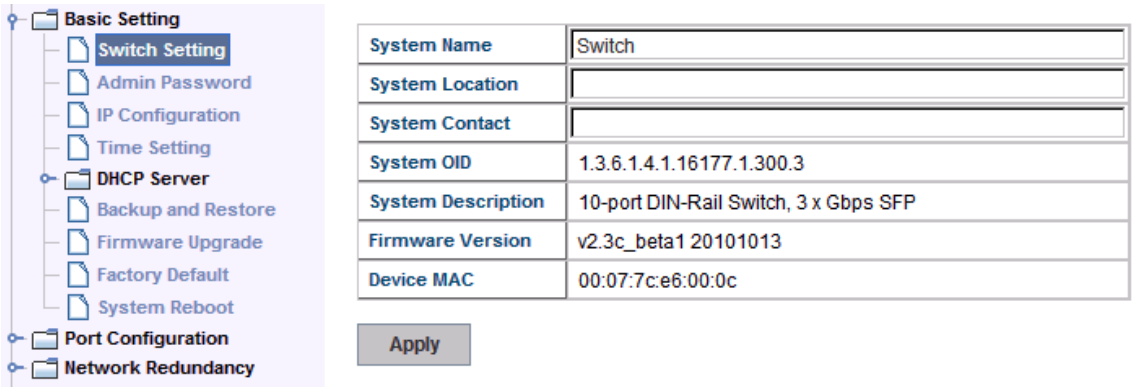
The Basic Setting group provides you to configure switch information, IP address, user name/password of the system. It also allows you to do firmware upgrade, backup and restore configuration, reload factory default, and reboot the system.

Following commands are included in this section:

4.2.1 Switch Setting

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

Figure 4.2.1.1 – Web UI of the Switch Setting



System Name: You can assign a name to the switch. The number of 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 number of 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 switch.

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

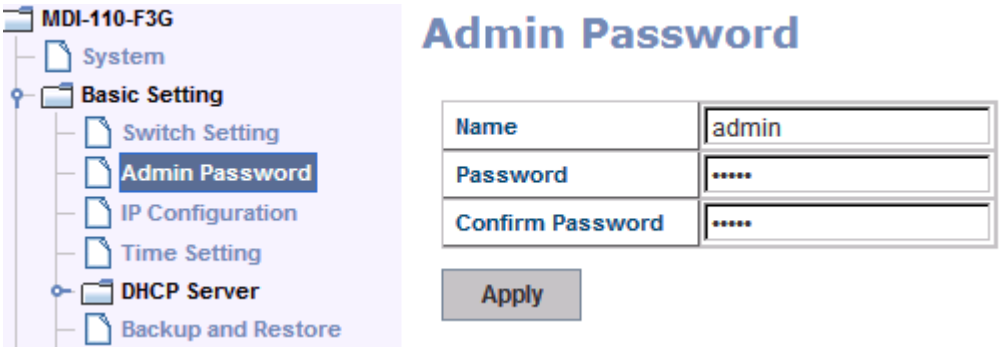


Figure 4.2.2.1 Web UI of the Admin Password

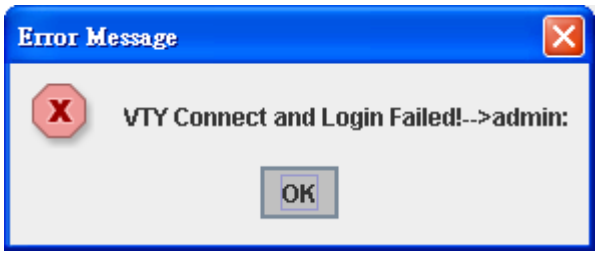
User name: You can type in a new user name here. The default setting is **admin**.

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.

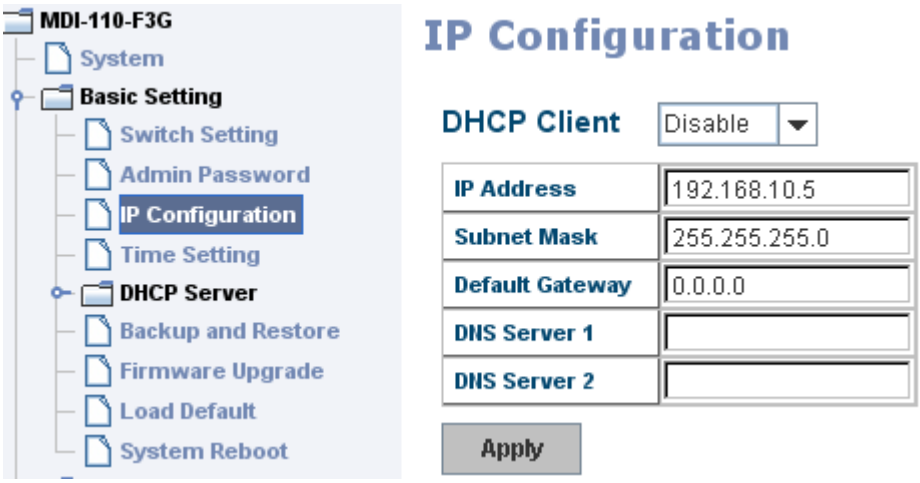
Once you finish configuring the settings, click on **Apply** to apply your configuration.

Figure 4.2.2.2 Popup alert window for incorrect user name.



4.2.3 IP Configuration

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



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.

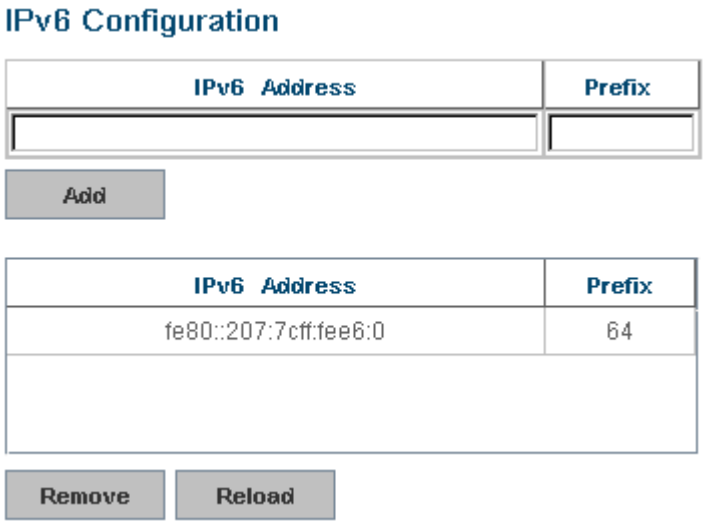
Once you finish configuring the settings, click on **Apply** to apply your configuration.

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.

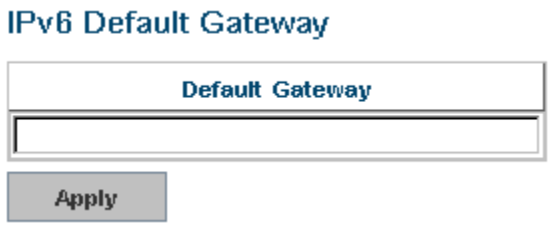
An example of an IPv6 address is: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

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:

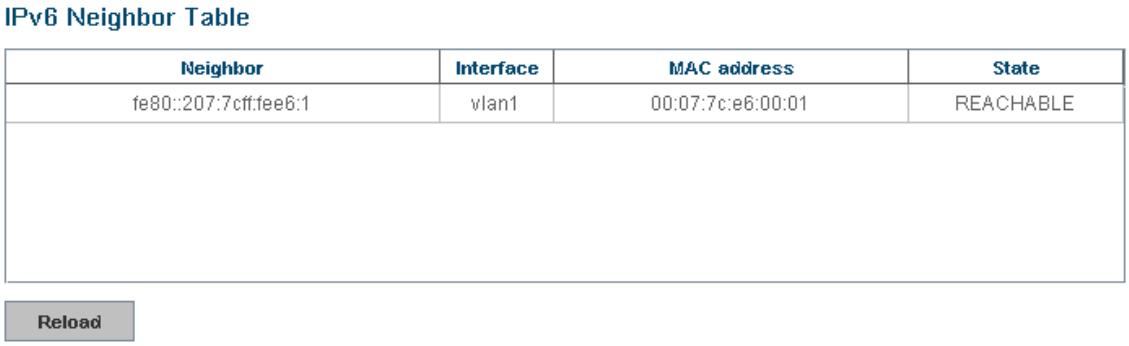
fe80::207:7cff:fe60:0.



IPv6 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.



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



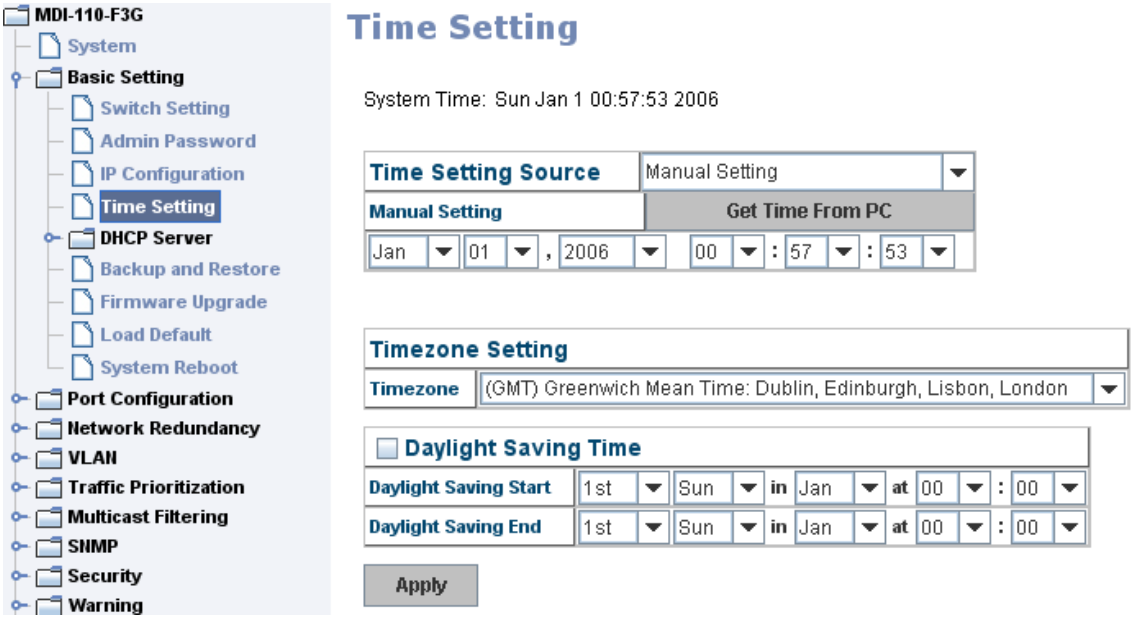
The system will update IPv6 Neighbor Table automatically, and user also can click the icon "**Reload**" to refresh the table.

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.



Manual Setting: User can select Manual setting to change time as user wants. User can click the button "Get Time from PC" to get PC's time setting for switch.

NTP client: Set Time Setting Source to NTP client to enable 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.

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

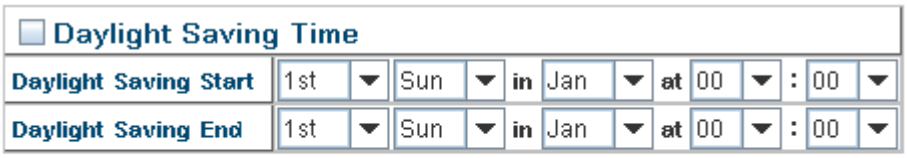
01 (GMT-12:00) Eniwetok, Kwajalein
02 (GMT-11:00) Midway Island, Samoa
03 (GMT-10:00) Hawaii
04 (GMT-09:00) Alaska
05 (GMT-08:00) Pacific Time (US & Canada) , Tijuana
06 (GMT-07:00) Arizona
07 (GMT-07:00) Mountain Time (US & Canada)
08 (GMT-06:00) Central America
09 (GMT-06:00) Central Time (US & Canada)
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 functions allows user to selects and apply the daylight saving start and end week by monthly basis.

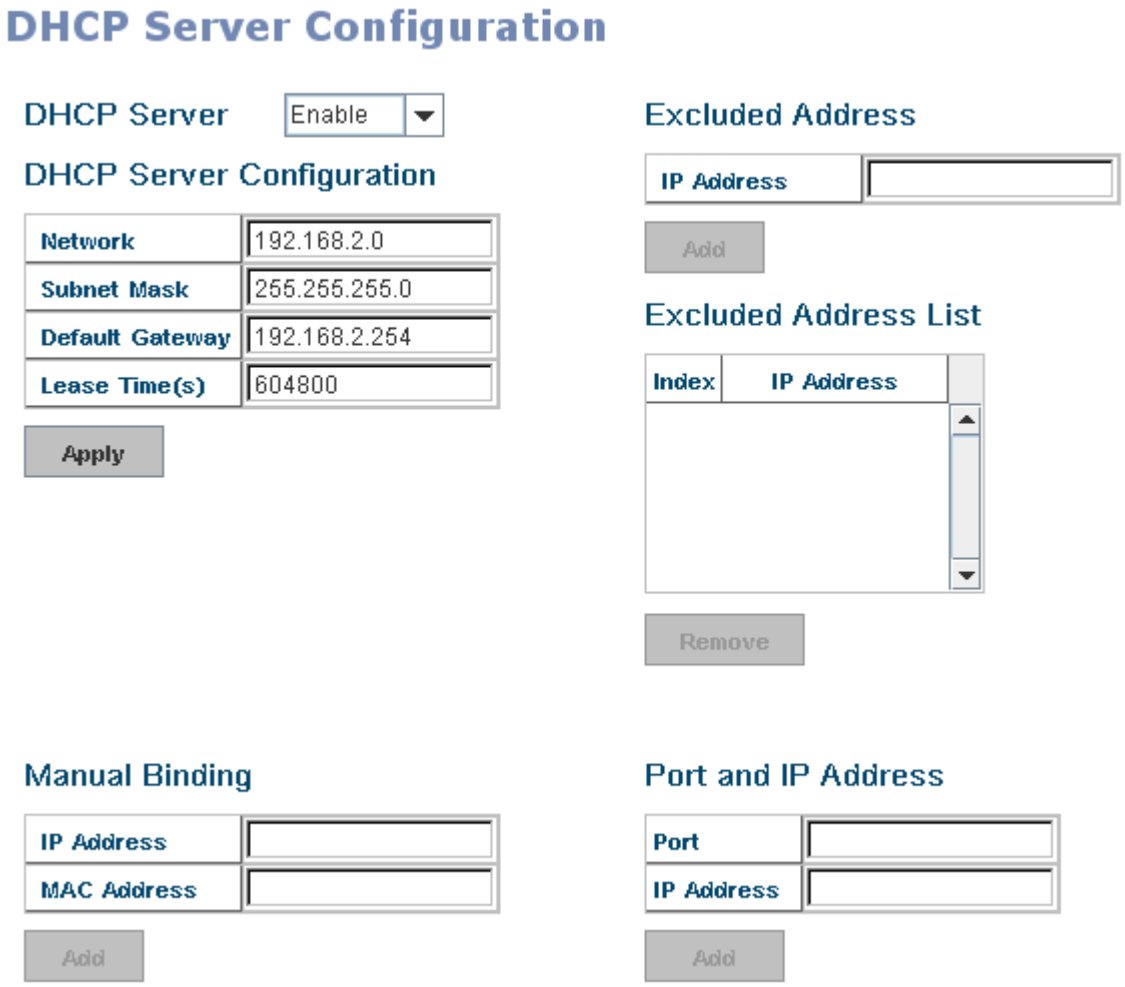


Once you finish your configuration, click on **Apply** to apply your configuration.

4.2.5 DHCP Server

You can select to **Enable** or **Disable** DHCP Server function. It will assign a new IP address to link partners, and also supports DHCP server option 82 with forwarding policy, and provides port-based DHCP server with IP address binding feature.

DHCP Server configuration



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.

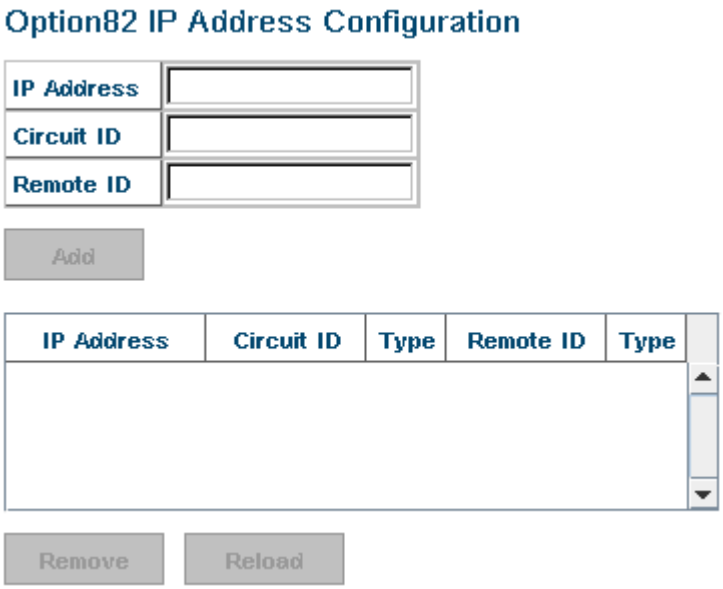
The IP address that is listed in the **Excluded Address List Table** will not be assigned to the network device. Add or remove an IP address from the **Excluded Address List** by clicking **Add** or **Remove**.

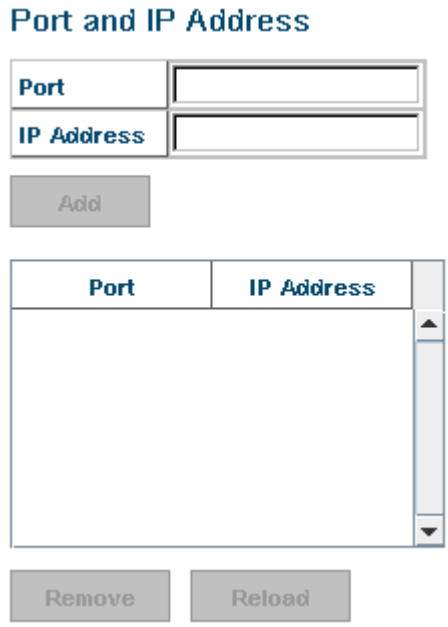
Manual Binding: the switch provides a MAC address and IP address binding and removing function. You can type in the specified IP and MAC address, then click **Add** to add a new MAC&IP address binding rule for a specified link partner, like PLC or any device without **DHCP client** function. To remove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

Option 82 IP Address Configuration: the DHCP server with option 82 function presented in latest firmware. This feature support fully DHCP relay function, and allows user to configured relay circuit ID, Remote ID to compliant fully DHCP

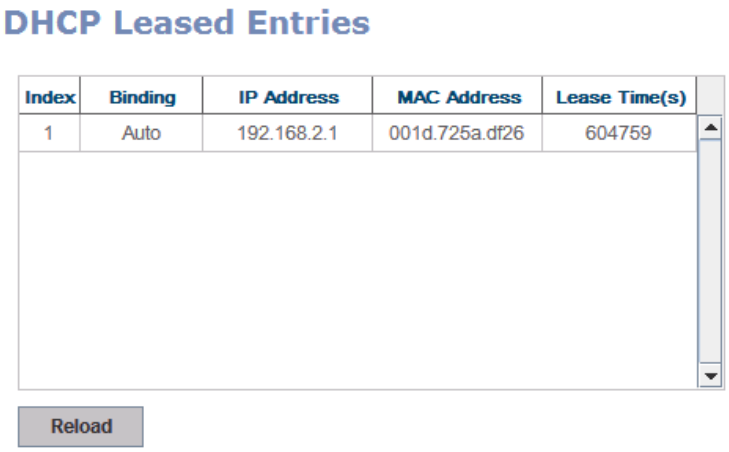
option 82 function.

Port and IP Address (Port Based DHCP Server configuration): the Switch also supports port-based DHCP server function. It allows user assign specified IP address to specified port that DHCP client presented; and the DHCP server only offer the predefined IP address to the DHCP client.



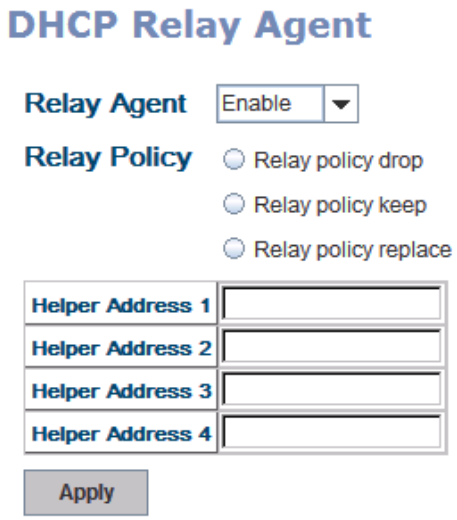


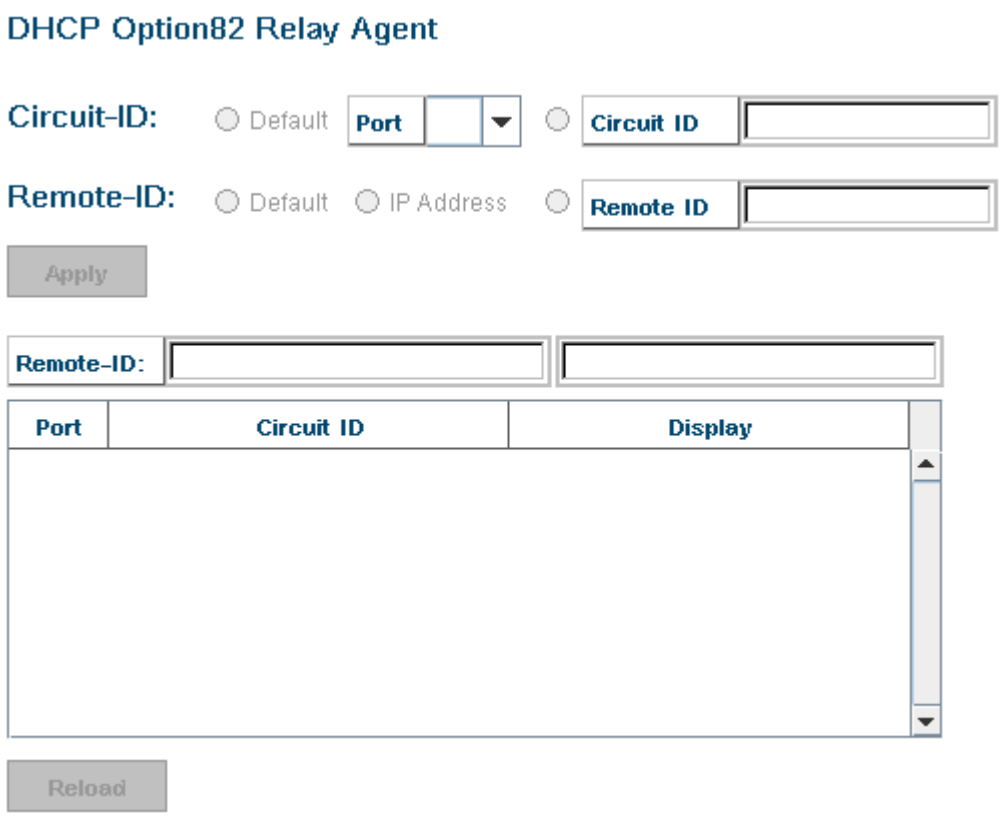
DHCP Leased Entries: the switch provides an assigned IP address list for user check. It will show the MAC and IP address that was assigned by the switch. Click the **Reload** button to refresh the listing.



DHCP Relay Agent

You can select to **Enable** or **Disable** DHCP relay agent function, and then select the modification type of option 82 field, circuit ID, remote ID.





Relay policy drop: Drops the option 82 field and do not add any option 82 field.

Relay policy keep: Keeps the original option 82 field and forwards to server.

Relay policy replace: Replaces the existing option 82 field and adds new option 82 field. (This is the default setting)

Helper Address: there are 4 fields for the DHCP server's IP address. You can filll the field with prefered IP address of DHCP Server, and then click "Apply" to activate the DHCP relay agent function. All the DHCP packets from client will be modified by the policy and forwarded to DHCP server through the gateway port.

4.2.6 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.

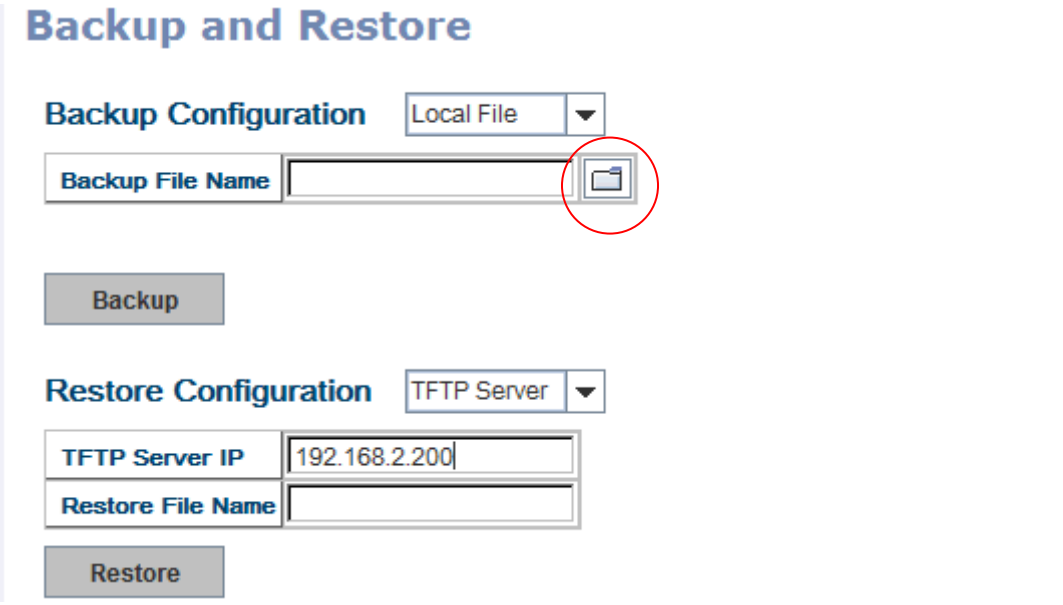
Backup/Restore File Name: Please type the correct file name of the configuration file.

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 CLI can show you the latest settings that are running on the system. The information shown here are 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



 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.

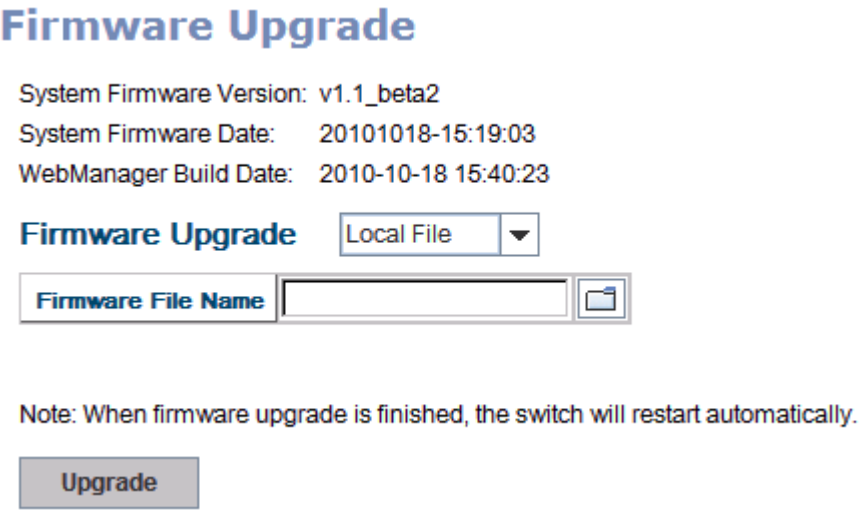
Type the IP address of TFTP Server IP. Then click on **Backup/Restore**.

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

4.2.7 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.



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 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.

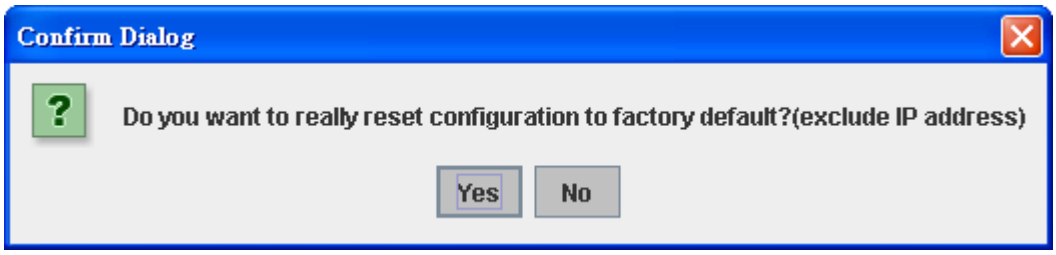
Click on **Upgrade** to start the process.

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.

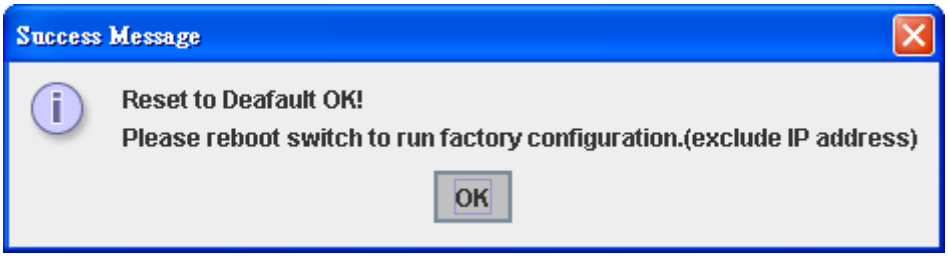
4.2.8 Factory Default

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.



Popup message screen to show you that have done the command. Click on **OK** to close the screen. Then please go to **Reboot** page to reboot the switch.



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

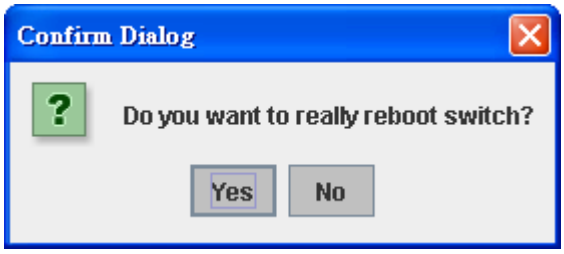
Note: If you already configured the IP of your device to other IP address, when you use this command by CLI and Web UI, our software will not reset the IP address to default IP. The system will remain the IP address so that you can still connect the switch via the network.

4.2.9 System Reboot

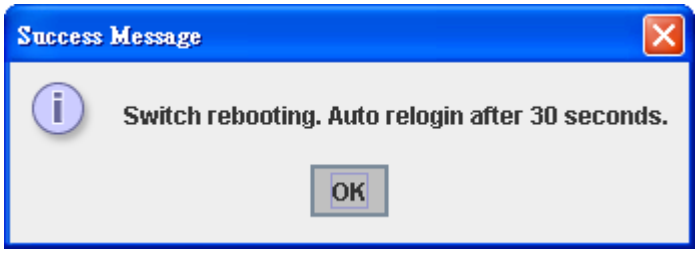
System Reboot allows you to reboot the device. Some of the feature changes require you to reboot the system. Click on **Reboot** to reboot your device.

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.



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



4.2.10 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 0.31-20061218 Switch# show hardware mac MAC Address : 00:07:7c:e6:00:00
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
	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 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.

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

DHCP Server	
DHCP Server configuration	Enable DHCP Server on Switch Switch# Switch# configure terminal Switch(config)# router dhcp Switch(config-dhcp)# service dhcp Configure DHCP network address pool

	Switch(config-dhcp)#network 192.168.17.0/24 -(network/mask) Switch(config-dhcp)#default-router 192.168.17.254
Lease time configure	Switch(config-dhcp)#lease 300 (300 sec)
DHCP Relay Agent	Enable DHCP Relay Agent Switch# Switch# configure terminal Switch(config)# router dhcp Switch(config-dhcp)# service dhcp Switch(config-dhcp)# ip dhcp relay information option Enable DHCP Relay policy Switch(config-dhcp)# ip dhcp relay information policy replace drop Relay Policy keep Drop/Keep/Replace option82 field replace
Show DHCP server information	Switch# show ip dhcp server statistics Switch# show ip dhcp server statistics DHCP Server ON Address Pool 1 network:192.168.17.0/24 default-router:192.168.17.254 lease time:300 Excluded Address List IP Address --------------- (list excluded address) Manual Binding List IP Address MAC Address --------------- -------------- (list IP & MAC binding entry) Leased Address List IP Address MAC Address Leased Time Remains --------------- -------------- --------------------

	(list leased Time remain information for each entry)
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 mdi-110.bin Firmware upgrading, don't turn off the switch! Tftping file mdi-110.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

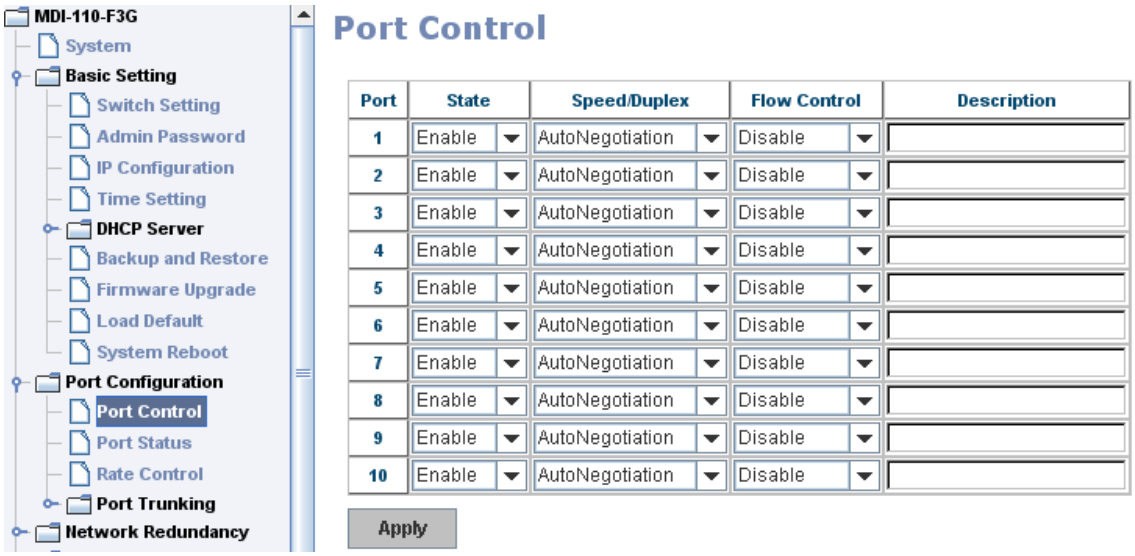
4.3 Port Configuration

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 section:

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.



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: AutoNegotiation, 10M Full Duplex(10 Full), 10M Half Duplex(10 Half), 100M Full Duplex(100 Full) and 100M Half Duplex(100 Half).

Gigabit Ethernet Port: AutoNegotiation, 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.

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.

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.

The switch supports SFP fiber transceiver with Digital Diagnostic Monitoring (DDM) function that provides real time information of SFP transceiver and allows user to diagnostic the optical fiber signal received and launched.

The information of SFP DDM will listing on another table.

Port Status

Port	Type	Link	State	Speed/Duplex	Flow Control	SFP Vendor	Wavelength	Distance
1	100BASE	Down	Enable	–	Disable	–	–	–
2	100BASE-TX	Up	Enable	100 Full	Disable	–	–	–
3	100BASE	Down	Enable	–	Disable	–	–	–
4	100BASE-TX	Up	Enable	100 Full	Disable	–	–	–
5	100BASE	Down	Enable	–	Disable	–	–	–
6	100BASE	Down	Enable	–	Disable	–	–	–
7	100BASE	Down	Enable	–	Disable	–	–	–
8	100BASE	Down	Enable	–	Disable	–	–	–
9	100BASE	Down	Enable	–	Disable	–	–	–
10	100BASE	Down	Enable	–	Disable	–	–	–

The description of the columns is as below:

Port: Port interface number.

Type: 100TX -> Fast Ethernet port. 1000TX -> Gigabit Ethernet 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.

Wavelength: The wave length of the SFP transceiver you plugged.

Distance: The distance of the SFP transceiver you plugged.

8	1000BASE	Down	Enable	--	Disable	--	--	--
9	1000BASE	Down	Enable	--	Disable	--	--	--
10	1000BASE-SX(DDM)	Down	Enable	--	Disable	WESTERMO i-...	1310nm	2000m

SFP DDM

Port	SFP Scan / Eject	SFP DDM	Temperature (°C)		Tx Power (dBm)		Rx Power (dBm)	
			Current	Range	Current	Range	Current	Range
8	Scan	Disable	--	--	--	--	--	--
9	Scan	Disable	--	--	--	--	--	--
10	Eject	Disable	40.00	-5.00 ~ 75.00	-5.6	-9.0 ~ -1.0	-40.0	-19.0 ~ -1.0

Reload | Scan All | Eject All

Reload: reload the all SFP port information.

Scan all: scan the SFP DDM transceiver and display the information.

Eject: Eject the SFP transceiver. You can eject one port or eject all by click the icon "Eject All".

Temperature: The temperature spcific and current detected of DDM SFP transceiver.

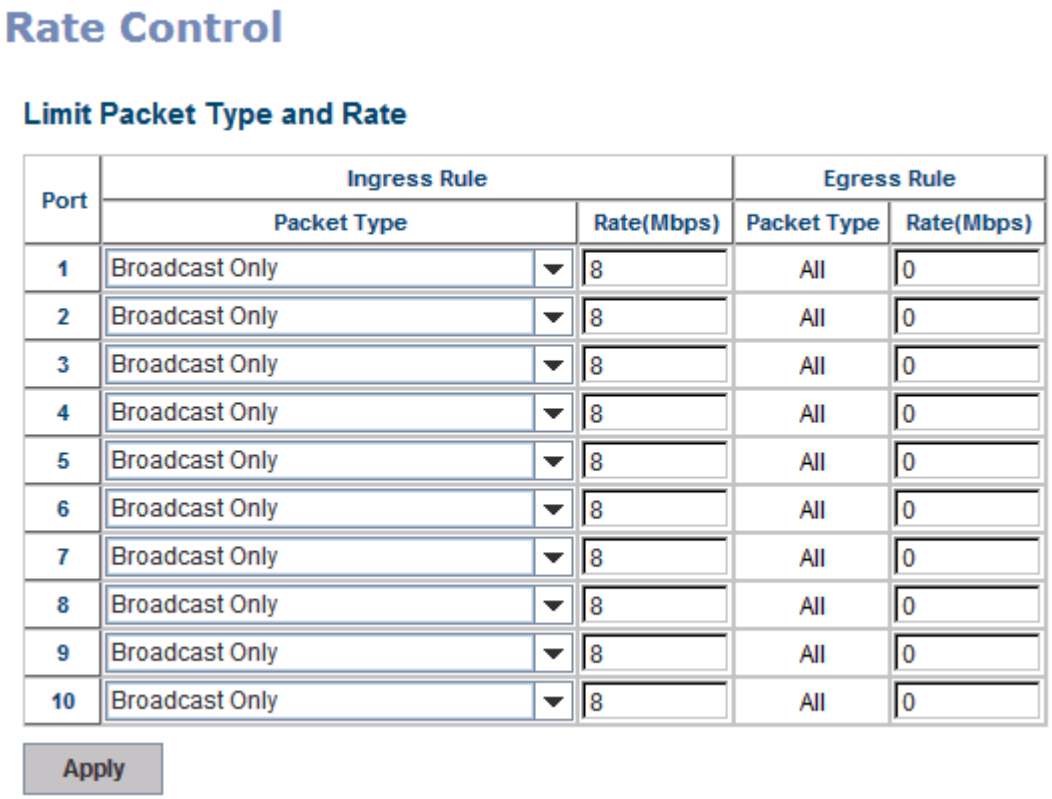
Tx Power (dBm): The specification and current transmit power of DDM SFP transceiver.

Rx Power (dBm): The specification and current received power of DDM SFP transceiver.

Note: **1. Most of the SFP transceivers provide vendor information which allows your switch to read it. The UI 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.**

2. if the plugged DDM SFP transceiver is not certified by Westermo, the DDM function will not be supported. But the communication will not be disabled.

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.

Packet type: You can select the packet type that you want to filter. The packet types of the Ingress Rule listed here include **Broadcast Only** / **Broadcast and multicast** / **Broadcast, Multicast and Unknown Unicast** or **All**. The packet types of the Egress Rule (outgoing) only support **all** packet types.

Rate: This column allows you to manually assign the limit rate of the port. Valid values are from 1Mbps-100Mbps for Fast Ethernet ports and Gigabit Ethernet ports. The step of the rate is 1 Mbps. Default value of Ingress Rule is “8” Mbps; default value of Egress Rule is 0 Mbps. The value 0 stands for disabling the rate control for the port.

Click on **Apply** to apply the configuration.

4.3.4 Port Trunking

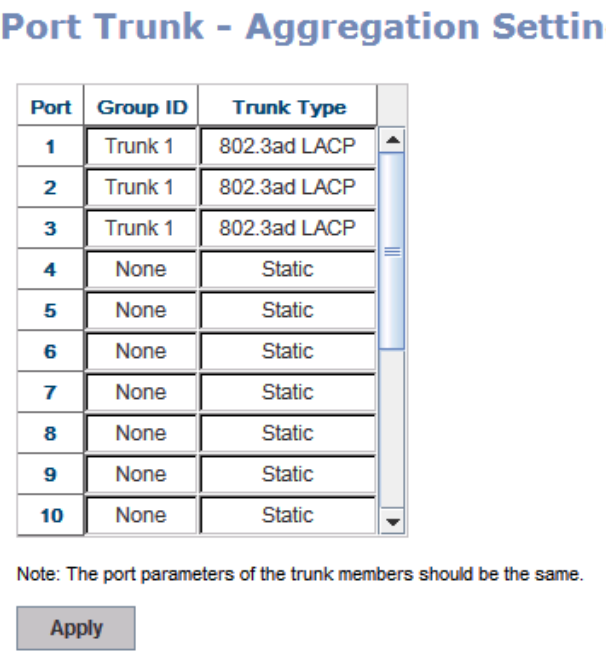
Port Trunking configuration allows you to group multiple Ethernet ports and to increase link bandwidth. The aggregated ports can be viewed as one physical port so that the bandwidth is higher than merely one single Ethernet port. The member ports of the same trunk group can balance the loading and backup 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. Westermo Supports two 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.

There are 2 configuration pages, Aggregation Setting and Aggregation Status.

Aggregation Setting



Trunk Size: The switch can support up to 5 trunk groups. Each trunk group can support up to 8 member ports. Since the member ports should use same speed/duplex, max groups for 100M ports would be 7, and 3 for gigabit ports.

Group ID: Group ID is the ID for the port trunking group. Ports with same group ID are in the same group.

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 of the specific port. LACP port priority is configured on each port using LACP. The port priority can be configured through the CLI. The higher the number, the lower the priority. The default value is 32768.

LACP Timeout: The LACPDU is generated and continue transmit within the LACP group. The interval time of the LACPDU Long timeout is 30 sec, this is default setting. The LACPDP Short timeout is 1 sec, the command to change from Long to Short is only applied to the CLI, the web GUI doesn't support this. Once the LACP port doesn't receive the LACPDP 3 times, that means the port may leave the group without earlier inform or does not detect 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, like the Wireless AP or Hub. 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 negotiated well, 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 5 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.

4.3.5 Command Lines for Port Configuration

Feature	Command Line
Port Control	
Port Control – State	Switch(config-if)# shutdown -> Disable port state Port1 Link Change to DOWN interface fastethernet1 is shutdown now. Switch(config-if)# no shutdown -> Enable port state Port1 Link Change to DOWN Port1 Link Change to UP interface fastethernet1 is up now. Switch(config-if)# Port1 Link Change to UP Switch(config)# sfp ddm Digital diagnostic and monitoring eject Eject SFP scan Scan SFP Switch(config)# sfp ddm enable Enable DDM disable Disable DDM Switch(config)# sfp ddm disable all → disable SFP DDM function on all SFP port Switch(config)# sfp eject all → eject all SFP transceiver Example: Switch(config)# sfp eject all SFP on Port 9 normally ejected. SFP on Port 10 normally ejected. All DDM SFP normally ejected.

	Switch(config)# interface gigabitethernet10 → eject port 10 SFP DDM transceiver. Switch(config-if)# sfp ddm eject DDM SFP on Port 10 normally ejected.
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 Port1 Link Change to DOWN set the speed mode ok! Switch(config-if)# Port1 Link Change to UP Switch(config-if)# duplex full Port1 Link Change to DOWN set the duplex mode ok! Switch(config-if)# Port1 Link Change to UP
Port Control – Flow Control	Switch(config-if)# flowcontrol on Flowcontrol on for port 1 set ok! Switch(config-if)# flowcontrol off Flow control 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 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. Switch# show sfp ddm →show SFP DDM information Port 8 Temperature:N/A Tx power:N/A Rx power:N/A Port 9 Temperature:64.00 C <range :0.0-80.00> Tx power:-6.0 dBm <range : -9.0 - -4.0> Rx power:-30.0 dBm <range: -30.0 - -4.0> Port 10 Temperature:67.00 C <range :0.0-80.00> Tx power:-6.0 dBm <range : -9.0 - -4.0> Rx power:-2.0 dBm <range: -30.0 - -4.0> 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 – Filter Packet Type	Switch(config-if)# rate-limit ingress mode all Limit all frames broadcast Limit Broadcast frames flooded-unicast Limit Broadcast, Multicast and flooded unicast frames multicast Limit Broadcast and Multicast frames Switch(config-if)# rate-limit ingress mode broadcast Set the ingress limit mode broadcast ok.
Rate Control –	Switch(config-if)# rate-limit ingress bandwidth

Bandwidth	<0-100> Limit in magabits per second (0 is no limit) Switch(config-if)# rate-limit ingress bandwidth 8 Set the ingress rate limit 8Mbps for Port 1.
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 Long/Short Timeout	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. Switch(config)# trunk group 2 fa6-7 Trunk group 2 enable ok!
Display - LACP	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) Switch# show trunk group 2 FLAGS: I -> Individual P -> In channel D -> Port Down Trunk Group GroupID Protocol Ports --------+---------+----------------------------------- 2 Static 6(D) 7(P) Switch#

4.4 Network Redundancy

The switch firmware supports standard STP/RSTP and Multiple Super Ring (MSR). The MSR includes Rapid Super Ring, Rapid Dual Homing, TrunkRing, MultiRing and backward compatible with Legacy Super Ring Client modes.

MDI-110 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 restoration 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:

The STP Configuration, STP Port Configuration and STP Information pages are available while select the STP and RSTP mode.

The MSTP Configuration, MSTP Port Configuration and MSTP Information pages are available while select the MSTP mode.

The Multiple Super Ring and Multiple Super Ring Information are available while

select the MSR mode.

The Switch supports port based STP Enable/disable function, and also provides loop protect for each port to achieve loop eliminate when applies STP and MSR functions.

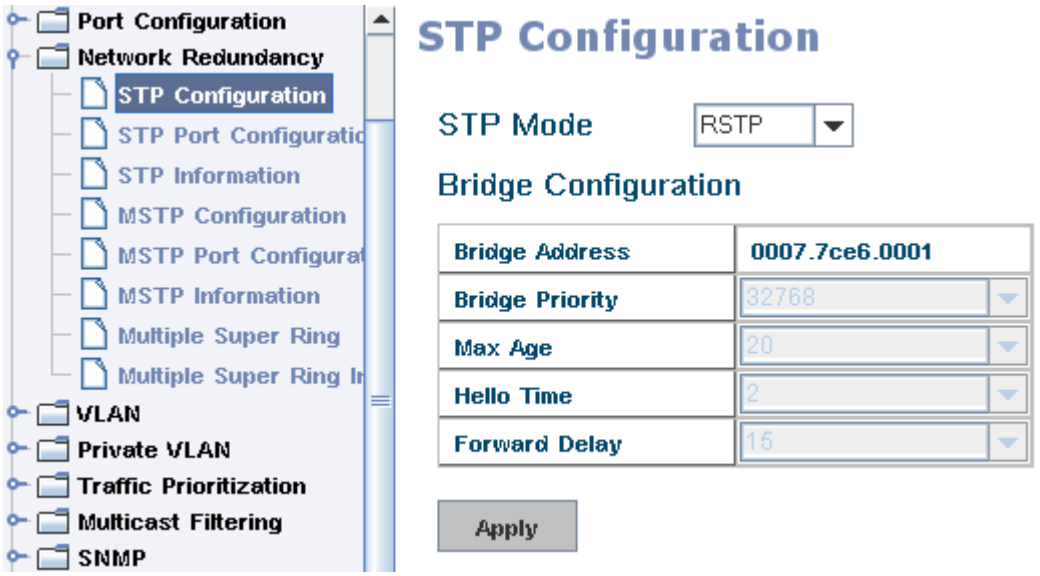
4.4.1 STP Configuration

This page allows select the STP mode and configuring the global STP/RSTP Bridge Configuration.

The STP mode includes the STP, RSTP, MSTP and Disable. Please select the STP mode for your system first. The default mode is RSTP enabled.

After select the STP or RSTP mode, continue to configure the global Bridge parameters for STP and RSTP.

After select the MSTP mode, please go to MSTP Configuration page.



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 damage 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 and 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).

Bridge Configuration

Bridge Address: This shows the switch's MAC address.

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.

Note: The Web GUI allows user select the priority number directly. This is the convenient of the GUI design. When you configure the value through the CLI or SNMP, you may need to type the value directly. Please follow the n x 4096 rules for the Bridge Priority.

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 the 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.

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 the switch will wait before checking to see if it should

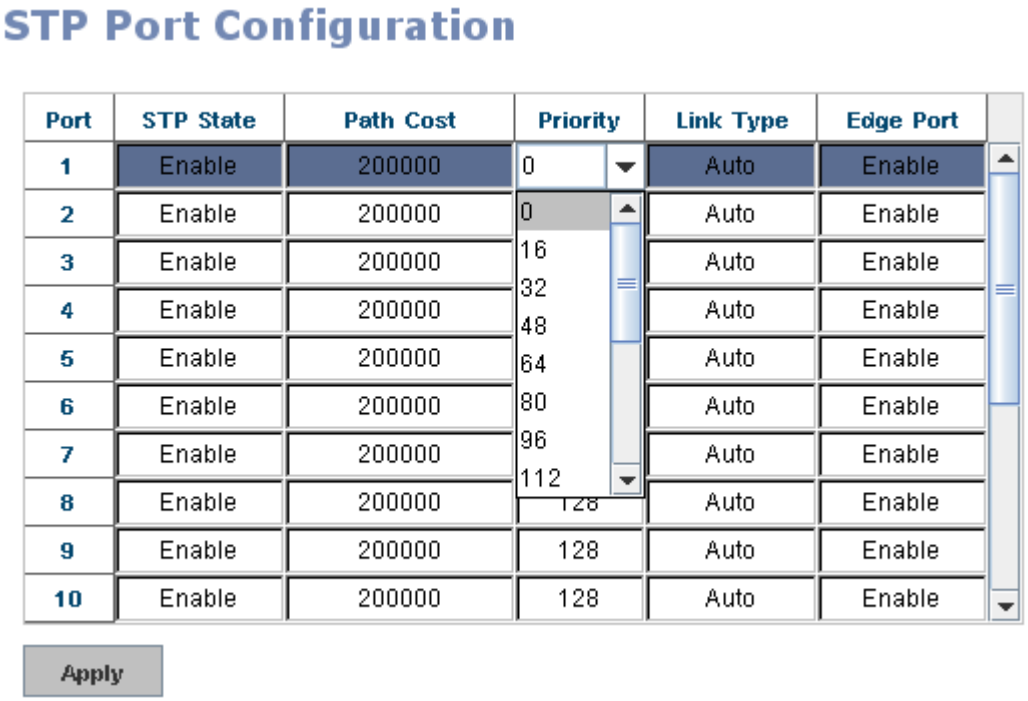
be changed to a different state.

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)

4.4.2 STP Port Configuration



This page allows you to configure the port parameter after enabled STP or RSTP.

Port Configuration

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

STP State: Enable /Disable the STP function by port configure.

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.

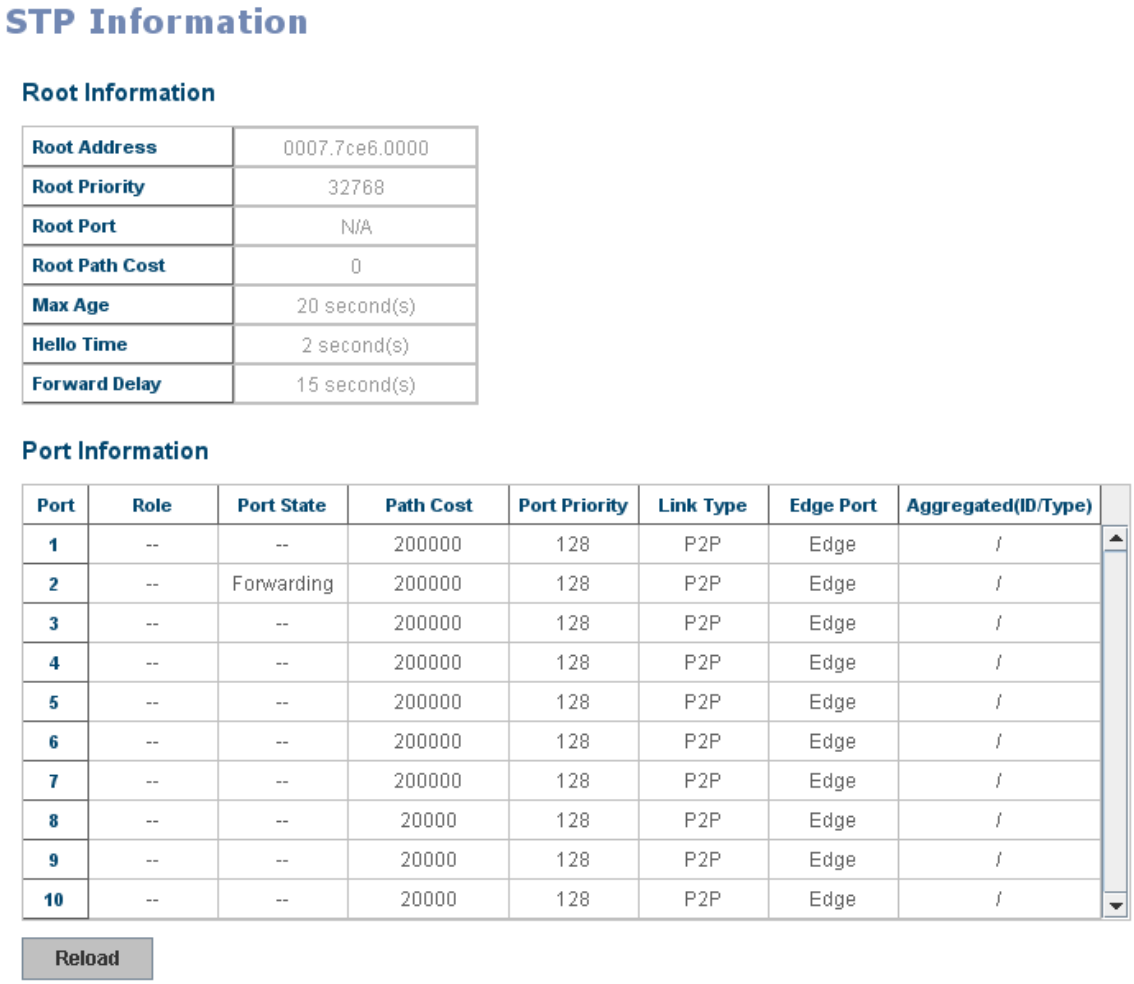
Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to another bridge (i.e. it is served by a point-to-point LAN segment), or if it can be connected to two or

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.

4.4.3 STP Info



STP Information

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	Aggregated(ID/Type)
1	--	--	200000	128	P2P	Edge	/
2	--	Forwarding	200000	128	P2P	Edge	/
3	--	--	200000	128	P2P	Edge	/
4	--	--	200000	128	P2P	Edge	/
5	--	--	200000	128	P2P	Edge	/
6	--	--	200000	128	P2P	Edge	/
7	--	--	200000	128	P2P	Edge	/
8	--	--	20000	128	P2P	Edge	/
9	--	--	20000	128	P2P	Edge	/
10	--	--	20000	128	P2P	Edge	/

Reload

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).

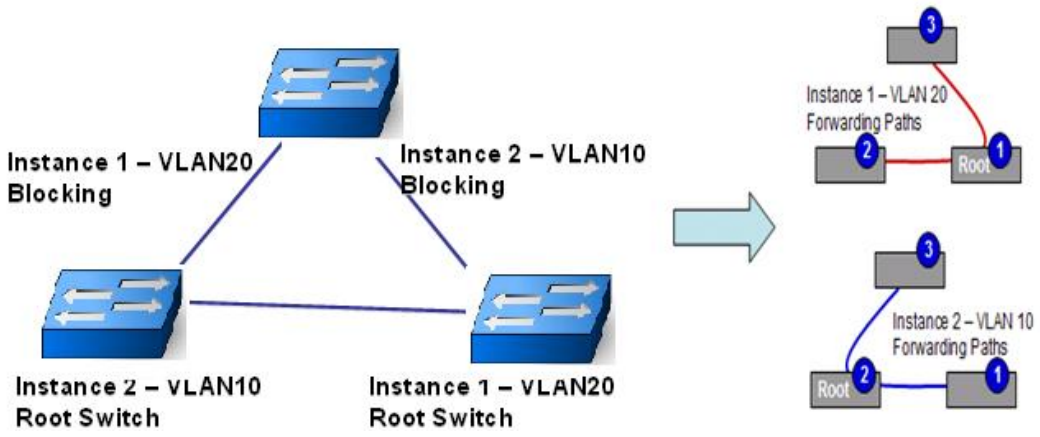
4.4.4 MSTP (Multiple Spanning Tree Protocol) Configuration

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.

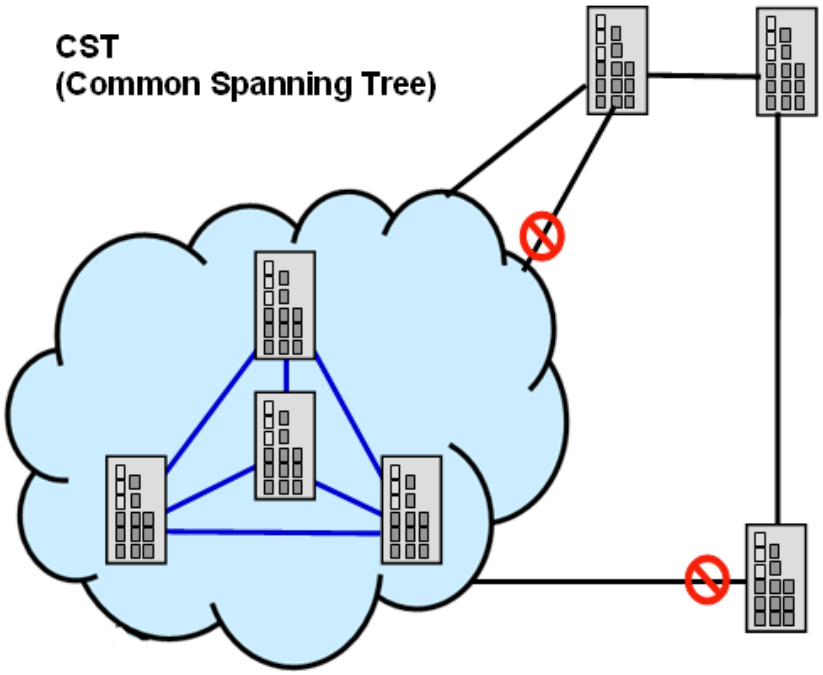
One VLAN can be mapped to a Multiple Spanning Tree Instance (MSTI). The maximum Instance Switch supports is 16, range from 0-15. The MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. An Internal Spanning Tree (IST) is 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.

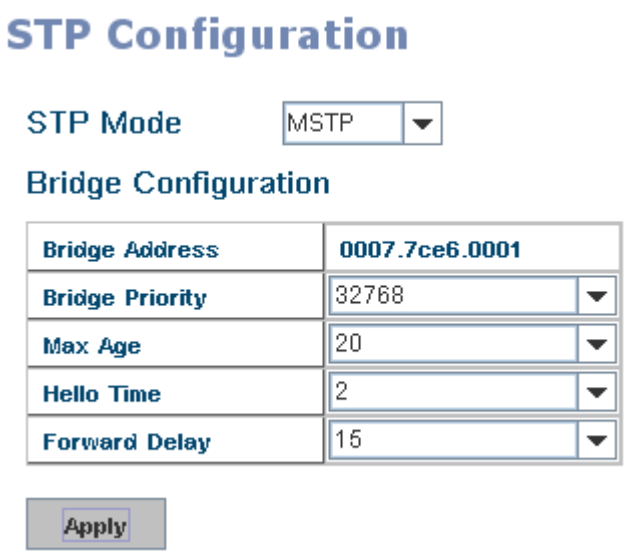


A Common Spanning Tree (CST) interconnects all adjacent MST regions and acts as a virtual bridge node for communications with STP or RSTP nodes in the global network. MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the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



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



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

MSTP Region Configuration

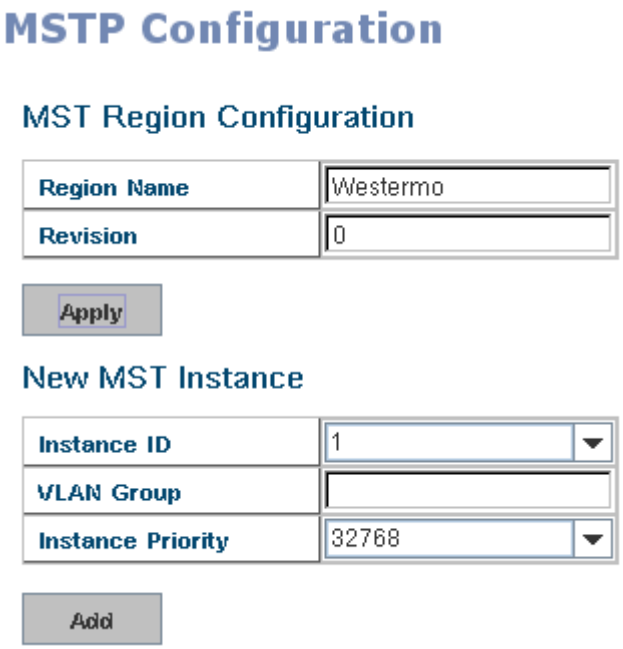
This page allows configure the Region Name and its Revision, mapping the VLAN to Instance and check current MST Instance configuration. The network can be divided virtually to different Regions. The switches within the Region should have the same Region and Revision level.

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.

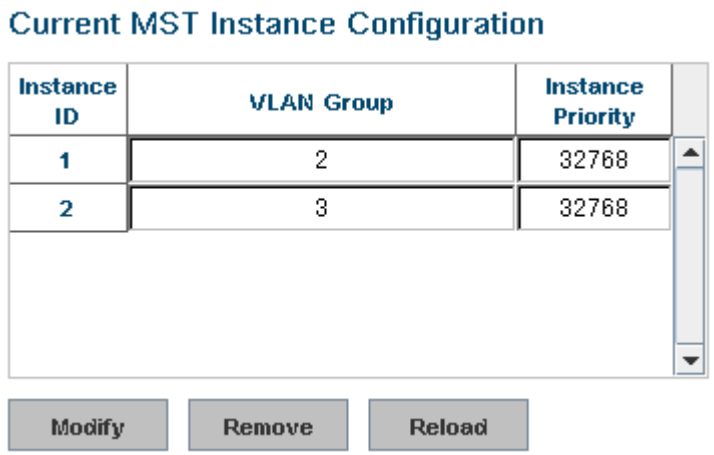
Instance ID: Select the Instance ID, the available number is 1-15.

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

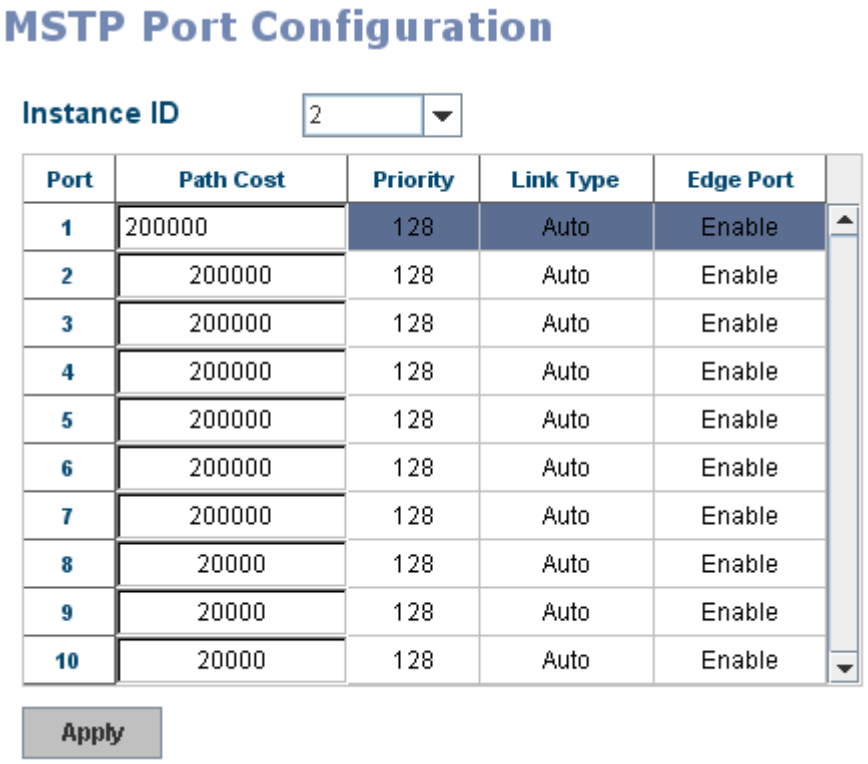


This page allows you to see the current MST Instance Configuration you added. Click on "**Apply**" to apply the setting. You can "**Remove"** the instance or "**Reload**" the configuration display in this page.

4.4.5 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.



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.

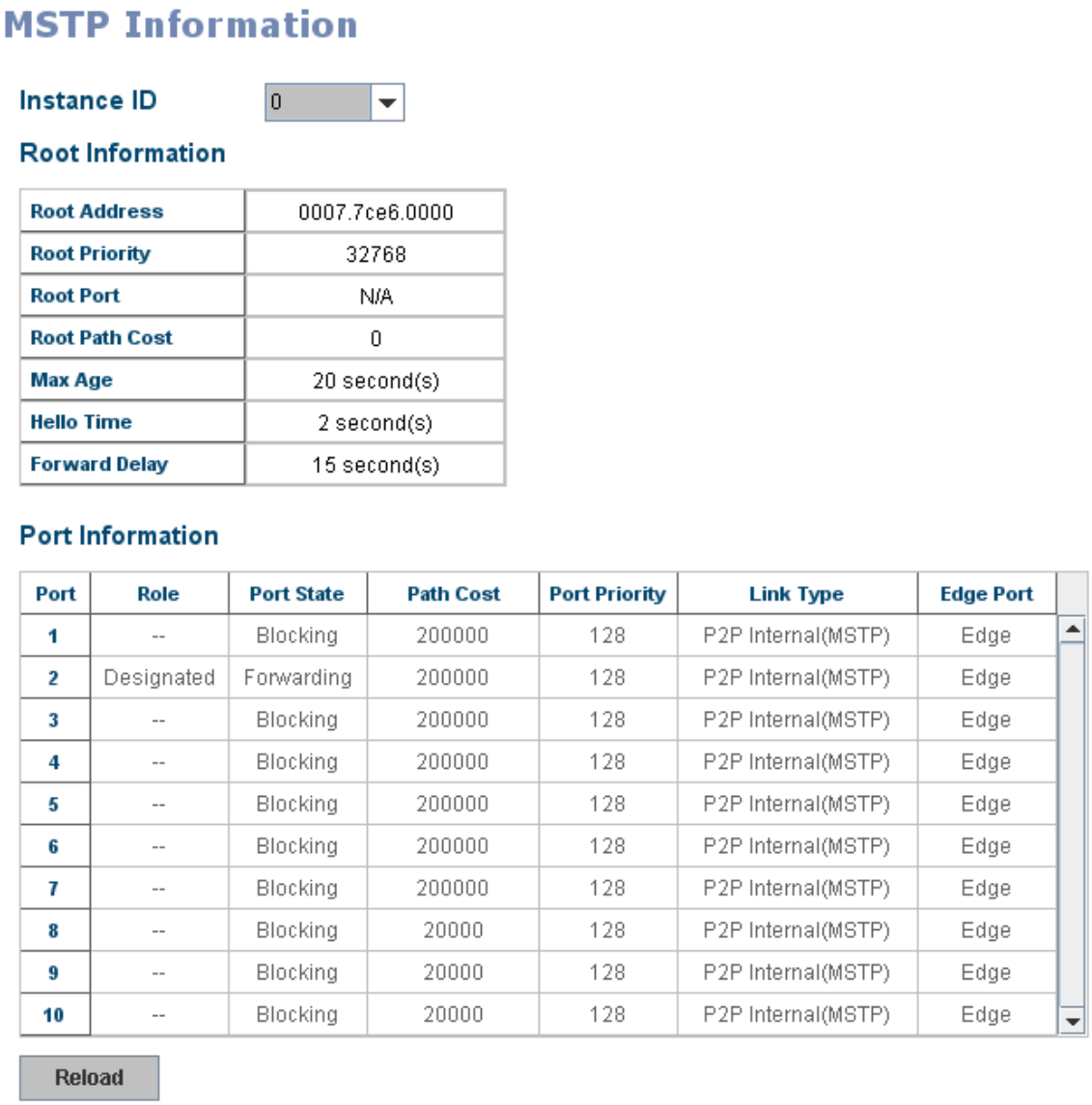
4.4.6 MSTP Information

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.



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

4.4.7 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 Korenix can support. 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 7+3G port design, that means maximum 5 Rings (4 x 100M Rings and 1 Gigabit Rings) can be aggregated to one &+3G Switch. The feature saves much effort when constructing complex network architecture.

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

Ring Configuration

ID: Once a Ring is created, this appears and can not be changed.

Name: 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”.

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

Device Priority: 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 a forwarding port and the other one will become a blocking port. If all of the switches have the same priority, the switch with the highest MAC address will be selected as Ring Master.

Ring Port1: In Rapid Super Ring environment, you should have two Ring Ports. No matter if the switch is Ring Master or not, when configuring RSR, two ports should be selected as 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 ring 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 loops. 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 pattern 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 JetNet 5428G.

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

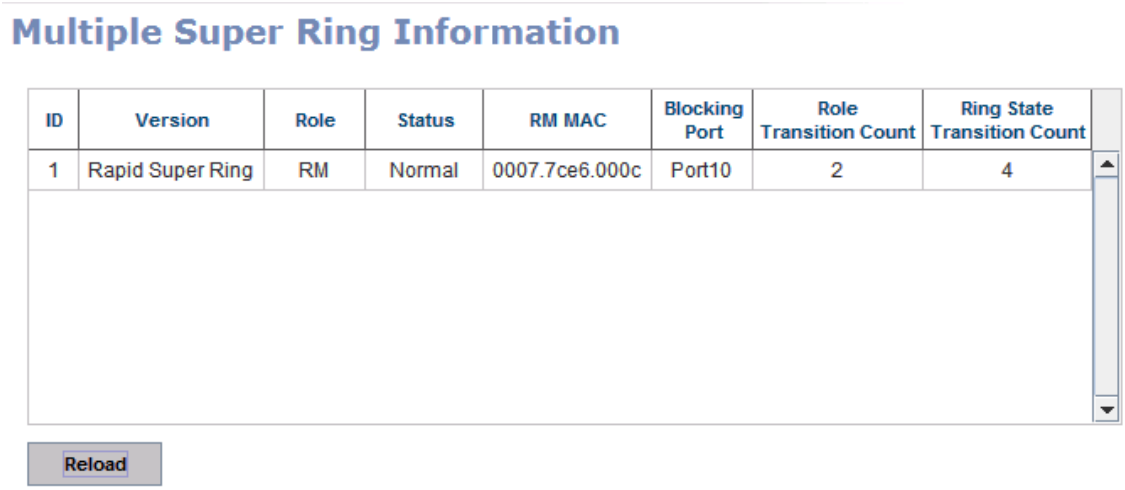
Technically, the maximum ring volume the MultiRing supported is up to 16 rings.

Due to the power 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 (stat 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.

4.4.8 Multiple Super Ring Info

This page shows the RSR information.



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.

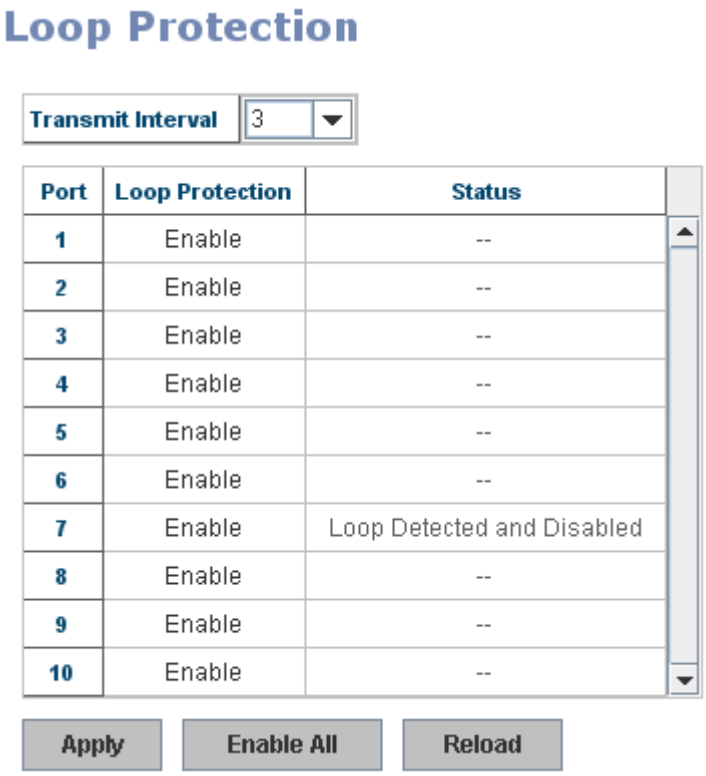
Blocking Port: This field shows which is blocked port of RM.

Role Transition Count: This means 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.

4.4.9 Loop Protection

The Switch supports loop eliminate function that based on per port or system configure, and prevents any looping caused by RSTP and MSR ring. The following figure shows the Loop Protect configuration.



Transmit interval: setting the detect duration time between detect packet.
Loop Protection: Enable/ Disable Loop Protection function by per port.
Status: shows the port status. If there is looping occurred, it will show "Loop Detected and Disabled" information and the link indicator will not turn-off, and also the port is disabled by system. **Once the looping is fixed, the blocked port will keep at blocked state, and must be enabled by manual or perform system reset to recovery it**.
Reload: refresh and update the port status information.

4.4.10 Command Lines:

Feature	Command Line
Global (STP, RSTP, MSTP)	
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 forward dleay 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)# name korenix 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 Configuraion	Switch(config-mst)# show current Current MST configuration Name [korenix] Revision 65535 Instance Vlans Mapped -------- --------------------------------------- 0 1,4-4094 1 2 2 3 --- 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	Switch(config-mst)# show pending

Configuration	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 2) --- 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 [korenix] (->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	
System RSTP Setting	The mode should be rst, the timings can be configured

	in global settings listed in above.
Port Configuration Mode	
Port Configuraiton	Switch(config)# interface fa1 Switch(config-if)# spanning-tree bpdufilter a secure BPDU process on edge-port interfcae bpduguard a secure response to invalid configurations(received BPDU sent by self) cost change an interafce's spanning-tree port path cost edge-port interface attached to a LAN segment that is at the end of a bridged LAN or to an end node link-type the link type for the Rapid Spanning Tree mst the multiple spanning-tree port-priority the spanning tree port priority
Port Path Cost	Switch(config-if)# spanning-tree cost <1-200000000> 16-bit based value range from 1-65535, 32-bit based value range from 1-200,000,000 Switch(config-if)# spanning-tree cost 200000
Port Priority	Switch(config-if)# spanning-tree port-priority <0-240> Number from 0 to 240, in multiple of 16 Switch(config-if)# spanning-tree port-priority 128
Link Type - Auto	Switch(config-if)# spanning-tree link-type auto
Link Type - P2P	Switch(config-if)# spanning-tree link-type point-to-point
Link Type – Share	Switch(config-if)# spanning-tree link-type shared
Edge Port	Switch(config-if)# spanning-tree edge-port enable Switch(config-if)# spanning-tree edge-port disable
MSTP Port Configuration	Switch(config-if)# spanning-tree mst MSTMAP cost <1-200000000> the value of mst instance port cost Switch(config-if)# spanning-tree mst MSTMAP port-priority <0-240> the value of mst instance port priority in multiple of 16
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 8 #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 0012.7700.0112 Designated bridge has priority 32768, address 0012.7760.1aec 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 [korenix] Revision 65535 Instance Vlans Mapped -------- --------------------------------------- 0 1,4-4094 1 2 2 3 --- 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
	  any-ring any ring auto detection
	  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.
Loop Protect	
loop-protect	Ethernet loop protection Switch(config)# loop-protect shows parameters of loop protect enable Enable loop protection disable Disable loop protection transmit-interval Set the transmission frequency of loop protection in seconds Switch(config)# loop-protect enable all

	Ethernet loop protection is enabled on all interfaces! Switch(config)# loop-protect transmit-interval <1-10> Valid range is 1~10 second(s) Switch(config)# loop-protect transmit-interval 3 →(set interval time – 3 seconds) Switch(config)# loop-protect enable fa6 → (fa1~7, gi7~gi10) Set fa6 Ethernet loop protection enabled! Switch# sh loop-protect →(show current loop-protect detected information) Loop protect information : Loop Protect Interface : fa6,gi10 Transmit Interval(sec) : 3 Loop Detected Interface : N/A

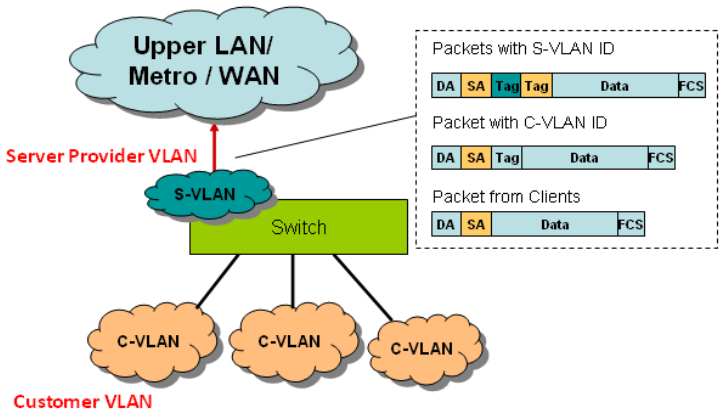
4.5 VLAN

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 (see Figure 1). 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 also 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 tag - 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 port Ingress/Egress parameters and view VLAN table.

Following commands are included in this section:

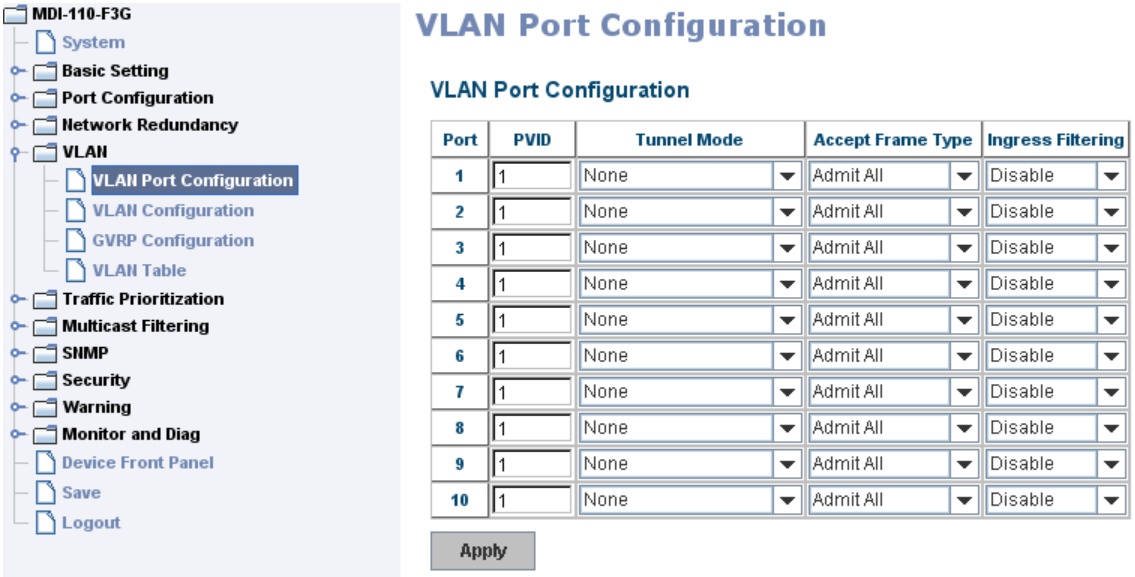
4.5.1 VLAN Port Configuration

4.5.2 VLAN Configuration

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.

Figure 4.5.2 Web UI of VLAN configuration.



PVID: The abbreviation of the **Port VLAN ID**. Enter the port 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. Value 1 is the default value and2 to 4094 are valid and available. **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.

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

The following are 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.

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.

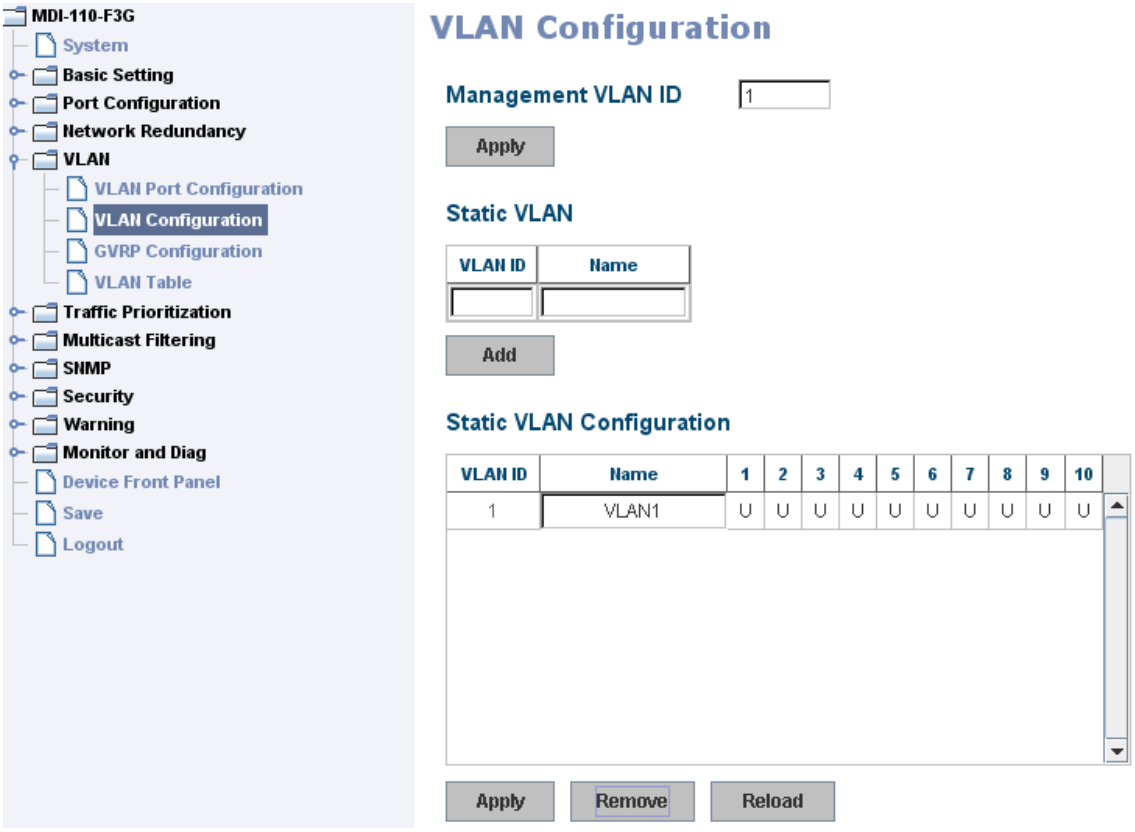
Ingress Filtering: Ingress filtering helps VLAN engine to filter out undesired traffic on a port. When Ingress Filtering is enabled, the port checks whether the incoming frames belong to the VLAN they claimed or not. Then the port determines if the frames can be processed or not. For example, if a tagged 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.

After 802.1Q Tunnel or 802.1Q Tunnel Uplink is enabled, the Ingress Filtering can not be configured.

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.

Figure 4.5.2.1 Web UI of the VLAN Configuration.



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 only support max 64 group VLAN.

Static VLAN Configuration

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

Figure 4.5.2.3 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.

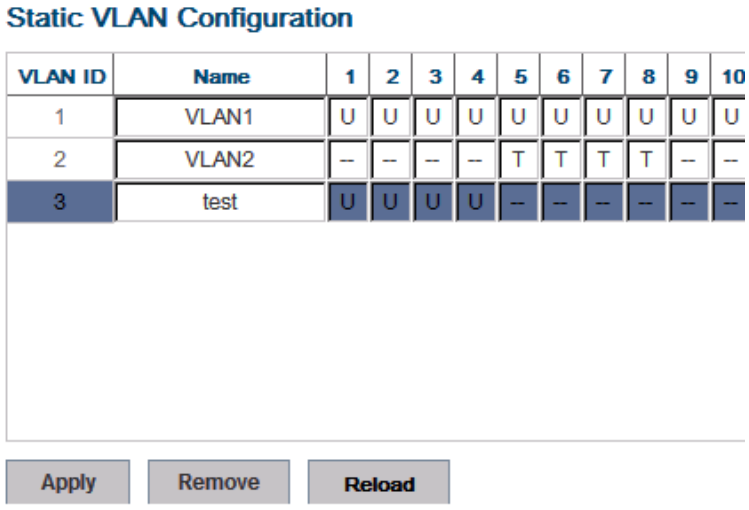


Figure 4.5.2.4 Configure Egress rule of the ports.

-- : Not available

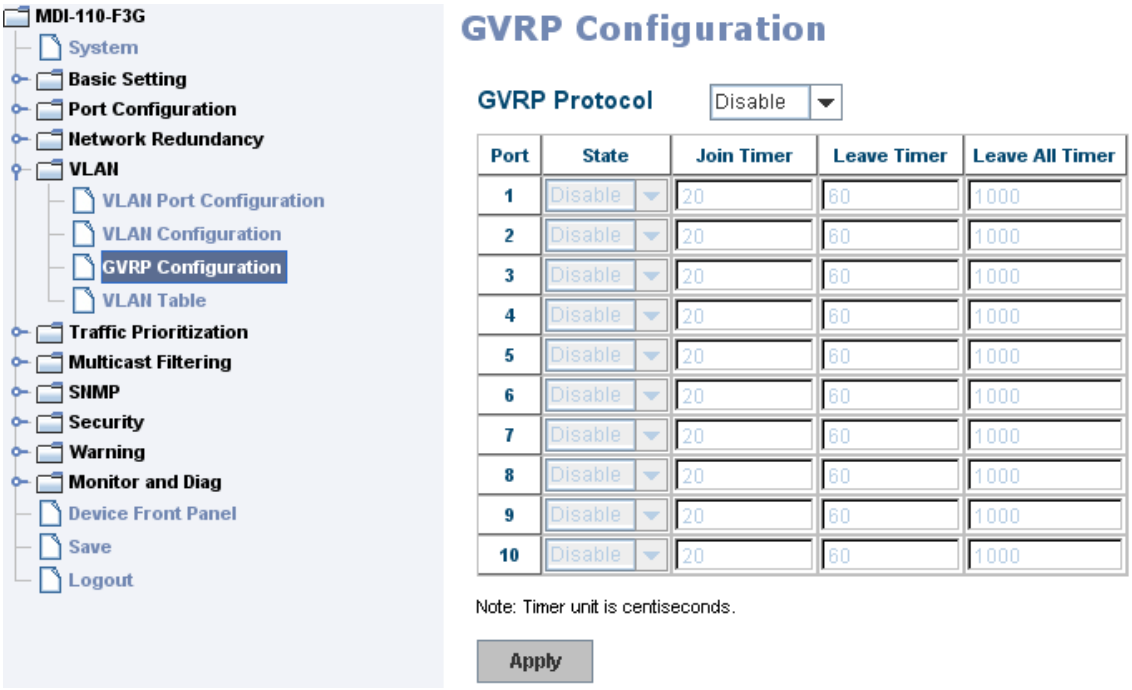
U: **Untag**: Indicates that egress/outgoing frames are not VLAN tagged.

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.



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

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

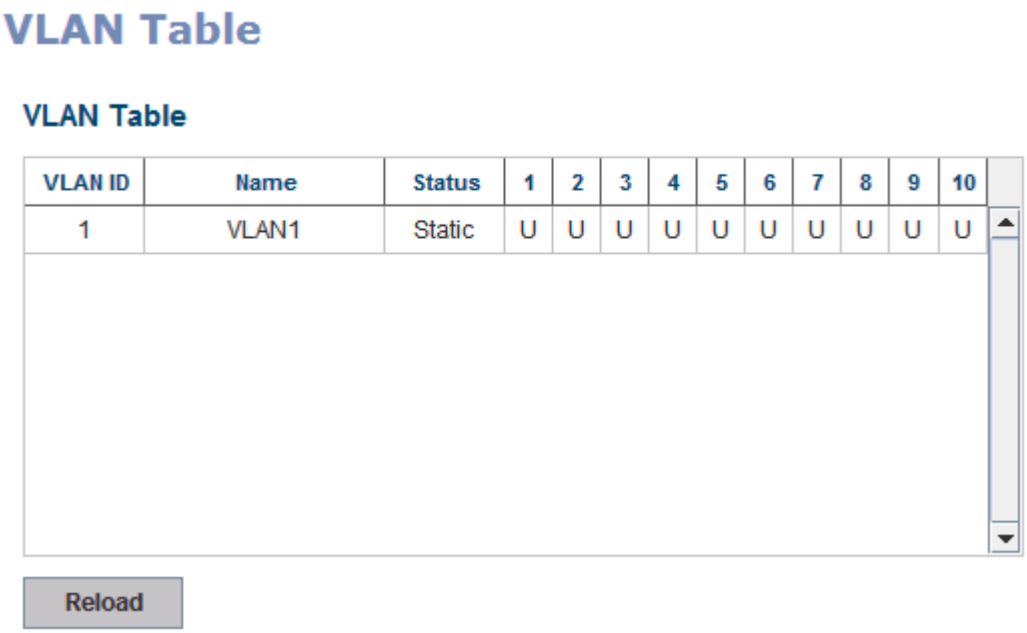
Join Timer: Controls the interval of sending the GVRP Join BPDU. An instance of this timer is required on a per-Port, per-GARP Participant basis

Leave Timer: Control the time to release the GVRP reservation after received the GVRP Leave BPDU and 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: 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 802.1Q Tunnel = access 802.1Q Tunnel Uplink = uplink	Switch(config-if)# switchport dot1q-tunnel mode Set the interface as an IEEE 802.1Q tunnel mode Switch(config-if)# switchport dot1q-tunnel mode 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-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-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	Switch# show interface fa1 Interface fastethernet1 Administrative Status : Enable Operating Status : Not Connected

Type)	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 192.168.10.8/24 no shutdown
QinQ Information – 802.1Q Tunnel	Switch# show dot1q-tunnel dot1q-tunnel mode port 1 : normal port 2 : normal port 3 : normal port 4 : normal port 5 : access port 6 : uplink port 7 : normal port 8 : normal port 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 192.168.10.18/24 Switch(config-if)# no ip address 192.168.10.8/24 ->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: 00:12:77:ff:01:b0 inet 192.168.10.100/24 broadcast 192.168.10.255

	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 192.168.10.17/24 ip igmp no shutdown ! ….

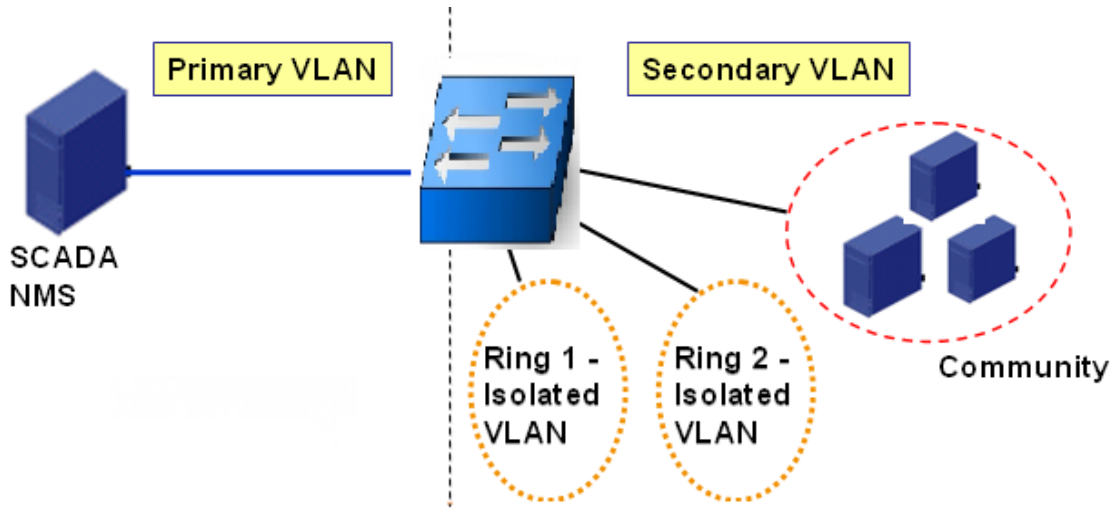
4.6 Private VLAN

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

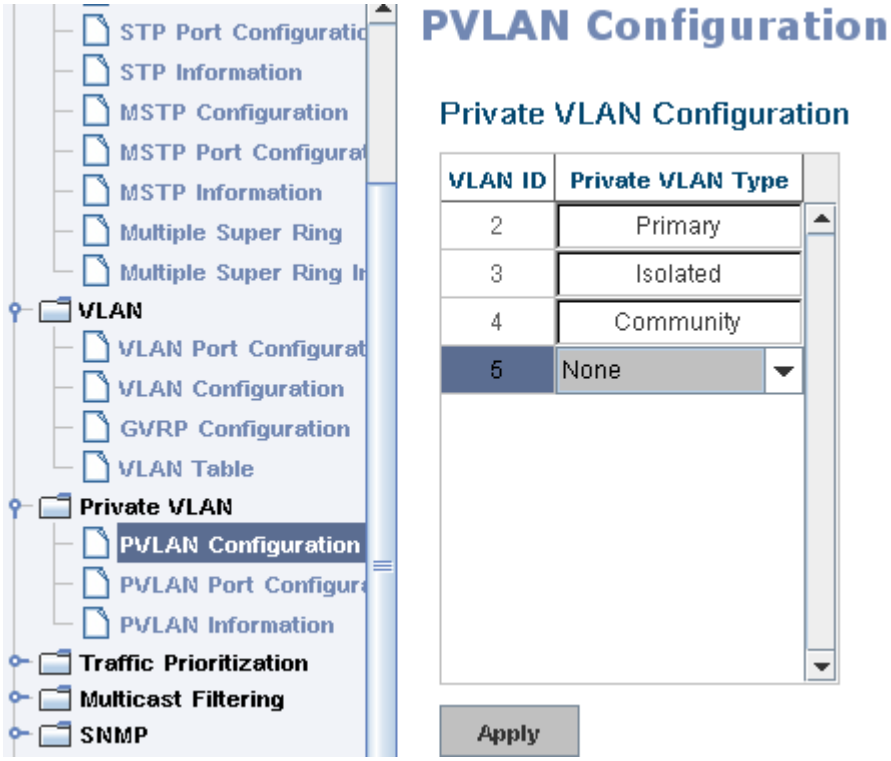
in VLAN Configuration page, the available VLAN ID will display here. Choose the Private VLAN types for each VLAN you want configure.

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.

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 Type :

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

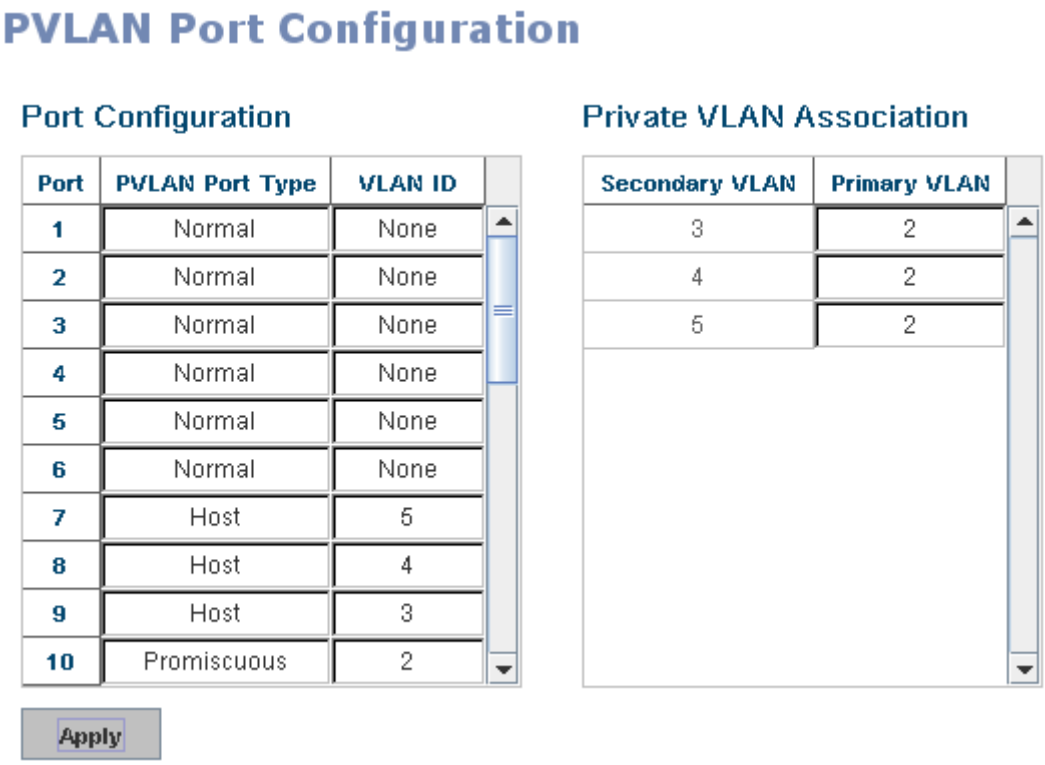
5. Result:

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..

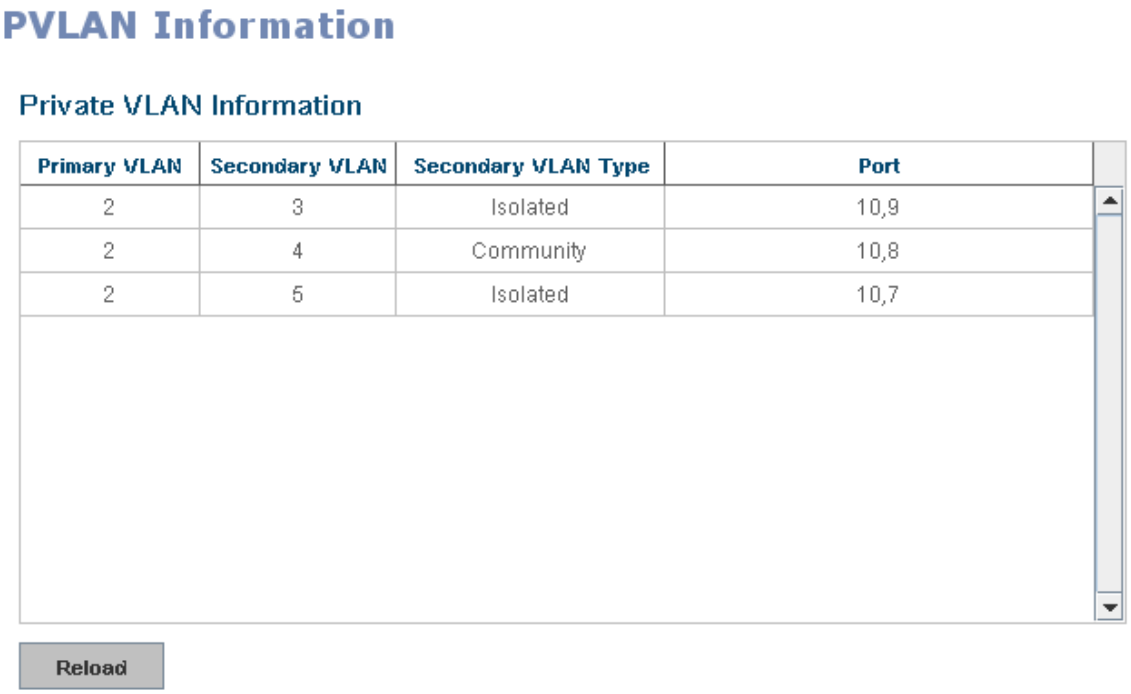
VLAN 4 -> VLAN 2, member ports within the community can communicate with each other and communicate with member port of VLAN 2.

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



4.6.3 Private VLAN Information

This page allows you to see the Private VLAN information.



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 Configuration	
Go to the port configuration	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	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

Host Port Type	Switch(config-if)# switchport mode private-vlan promiscuous <cr> Switch(config-if)# switchport mode private-vlan host <cr>
Private VLAN Port Configuration PVLAN Port Type Host Association primary to secondary (The command is only available for host port.)	Switch(config)# interface gi9 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 Private VLAN Type Private VLAN Port Information	Switch# show run Building configuration... Current configuration: hostname Switch vlan learning independent ! vlan 1 ! vlan 2 private-vlan primary ! vlan 3 private-vlan isolated ! vlan 4 private-vlan community ! vlan 5 private-vlan community ! …….. …….. 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 …… ……

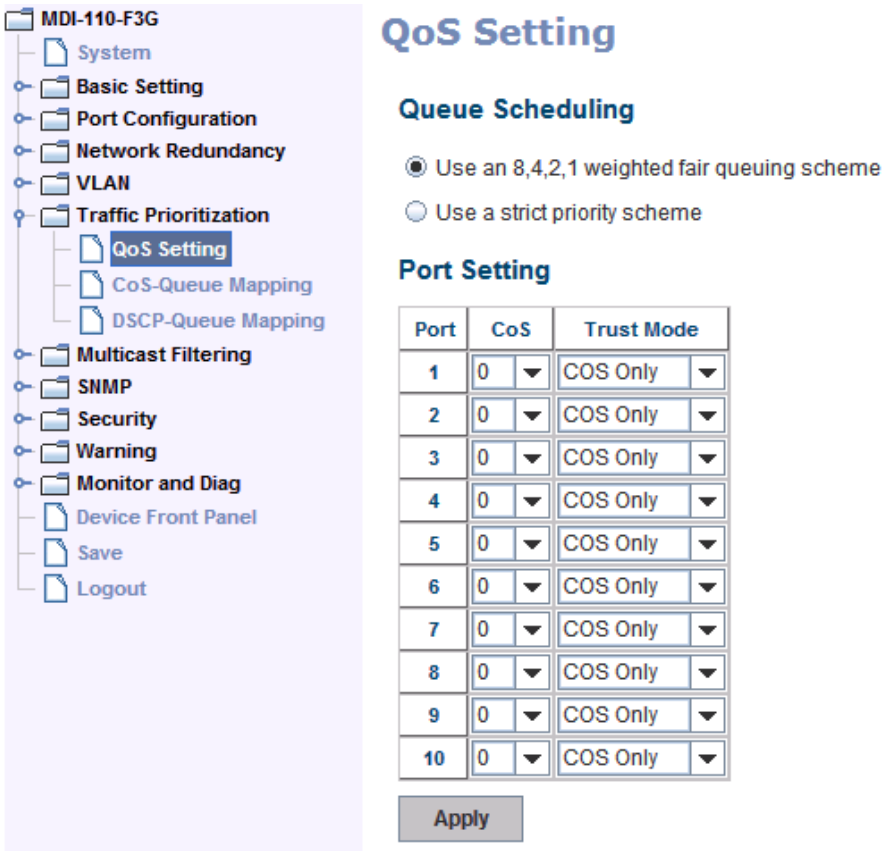
4.7 Traffic Prioritization

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.

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 section:

4.7.1 QoS Setting



Queue Scheduling

You can select the Queue Scheduling rule as follows:

Use an 8,4,2,1 weighted fair queuing scheme. This is also known as **WRR**

(Weight Round Robin)**.** The switch will follow 8:4:2:1 rate to process the packets in a queue from the highest priority to the lowest. For example, the system will process 8 packets with the highest priority in the queue, 4 with middle priority, 2 with low priority, and 1 with the lowest priority at the same time.

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.

Port Setting

CoS column is to indicate default port priority value for untagged or priority-tagged frames. When the switch receives the frames, it will attach the value to the CoS field of the incoming VLAN-tagged packets. You can enable 0,1,2,3,4,5,6 or 7 to the port.

Trust Mode is to indicate Queue Mapping types for you to select.

COS Only: Port priority will only follow COS-Queue Mapping you have assigned.

DSCP Only: Port priority will only follow DSCP-Queue Mapping you have assigned.

COS first: Port priority will follow COS-Queue Mapping first, and then DSCP-Queue Mapping rule.

DSCP first: Port priority will follow DSCP-Queue Mapping first, and then COS-Queue Mapping rule.

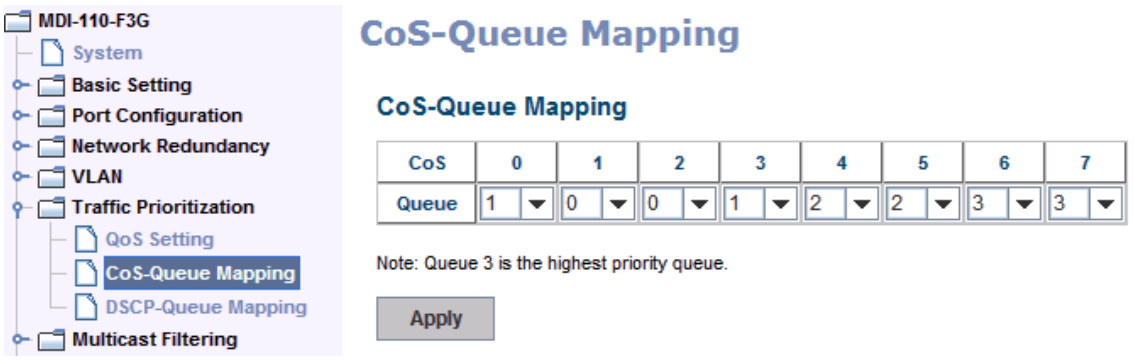
Default priority type is **COS Only**. The system will provide default COS-Queue table to which you can refer for the next command.

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

4.7.2 CoS-Queue Mapping

This page is to change CoS values to Physical Queue mapping table. Since the switch fabric 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.

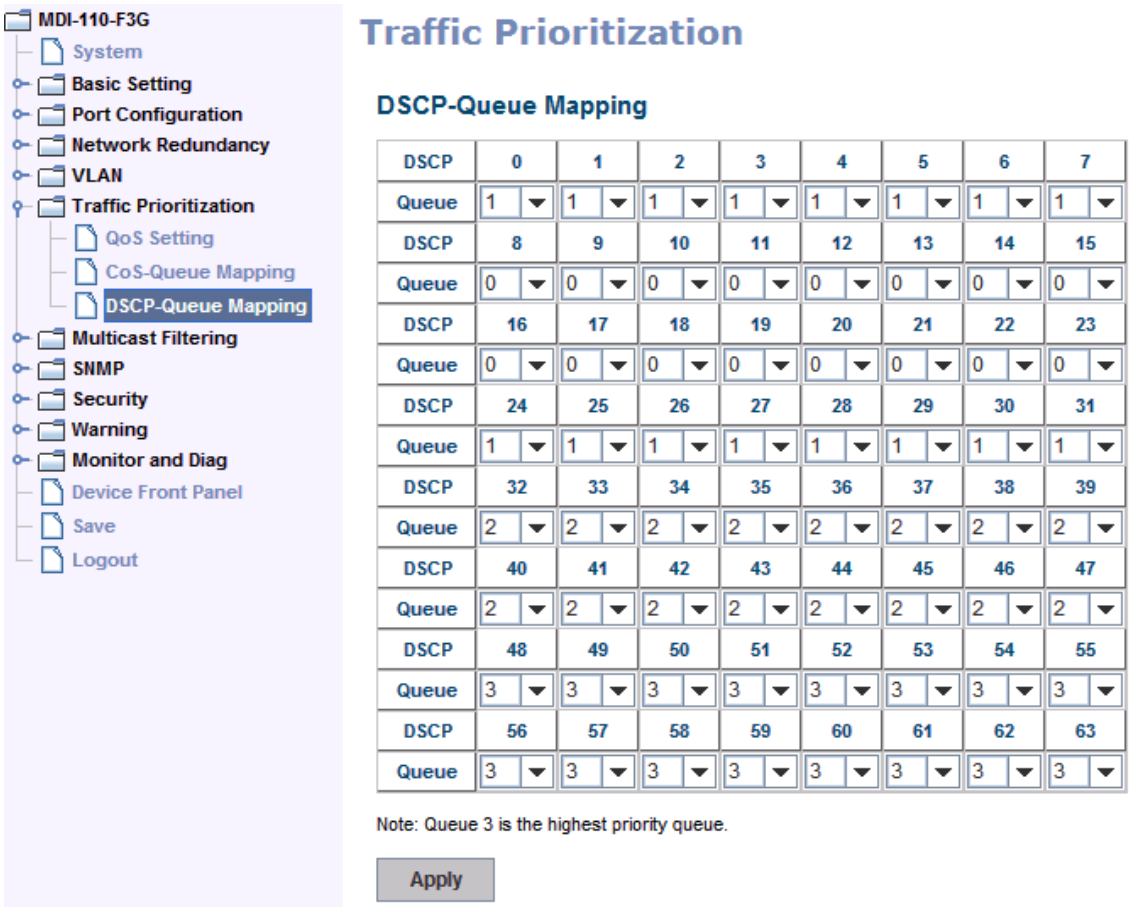
You can freely assign the mapping table or follow the suggestion of the 802.1p standard and Westermo uses 802.p suggestion as default values. You can find CoS values 1 and 2 are mapped to physical Queue 0, the lowest queue. CoS values 0 and 3 are mapped to physical Queue 1, the low/normal physical queue. 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.



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

4.7.3 DSCP-Queue Mapping

This page is to change DSCP values to Physical Queue mapping table. Since the switch fabric 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. You can freely change the mapping table to follow the upper layer 3 switch or routers' DSCP setting.



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

4.7.4 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 (Use an 8,4,2,1 weight) Switch(config)# qos queue-sched sp <cr>
Queue Scheduling - WRR	Switch(config)# qos queue-sched wrr
Port Setting – CoS (Default Port Priority)	Switch(config)# interface fa1 Switch(config-if)# qos cos DEFAULT-COS Assign an priority (7 highest) Switch(config-if)# qos cos 7 The default port CoS value is set 7 ok. Note: When change the port setting, you should Select the specific port first. Ex: fa1 means fast Ethernet port 1.
Port Setting – Trust Mode- CoS Only	Switch(config)# interface fa1 Switch(config-if)# qos trust cos The port trust is set CoS only ok.
Port Setting – Trust Mode- CoS First	Switch(config)# interface fa1 Switch(config-if)# qos trust cos-first The port trust is set CoS first ok.
Port Setting – Trust Mode- DSCP Only	Switch(config)# interface fa1 Switch(config-if)# qos trust dscp The port trust is set DSCP only ok.
Port Setting – Trust Mode- DSCP First	Switch(config)# interface fa1 Switch(config-if)# qos trust dscp-first The port trust is set DSCP first ok.
Display – Queue Scheduling	Switch# show qos queue-sched QoS queue scheduling scheme : Weighted Round Robin (Use an 8,4,2,1 weight)
Display – Port Setting - Trust Mode	Switch# show qos trust QoS Port Trust Mode : Port Trust Mode

	-----+------------ 1 DSCP first 2 COS only 3 COS only 4 COS only 5 COS only 6 COS only 7 COS only 8 COS only 9 COS only 10 COS only
Display – Port Setting – CoS (Port Default Priority)	Switch# show qos port-cos Port Default Cos : Port CoS -----+---- 1 7 2 0 3 0 4 0 5 0 6 0 7 0 8 0 9 0 10 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 6 3 7 3
DSCP-Queue Mapping	
Format	Switch(config)# qos dscp-map PRIORITY Assign an priority (63 highest) Switch(config)# qos dscp-map 0 QUEUE Assign an queue (0-3) Format: qos dscp-map priority_value queue_value
Map DSCP 0 to Queue 1	Switch(config)# qos dscp-map 0 1 The TOS/DSCP to queue mapping is set ok.

Display – DSCO-Queue mapping	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 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

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 Force Filtering

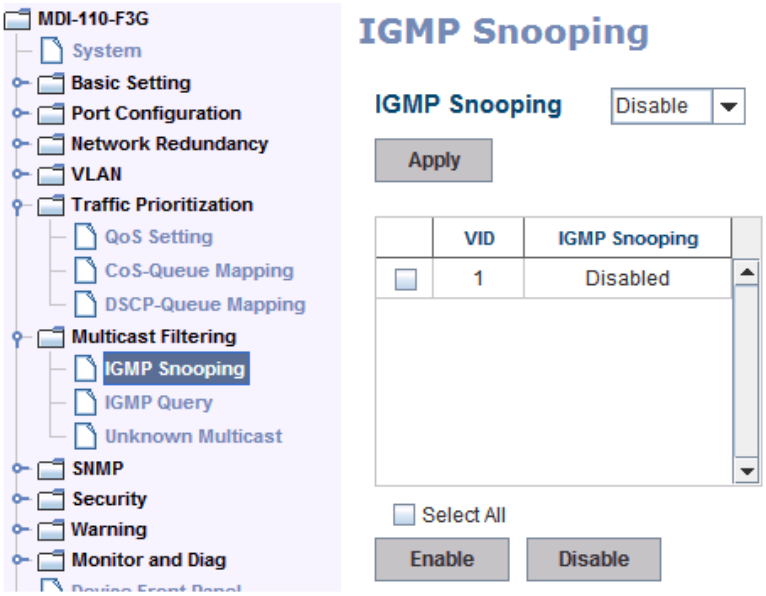
4.8.4 CLI Commands of the Multicast Filtering

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 supports IGMP snooping V1/V2/V3 automatically and IGMP query V1/V2.

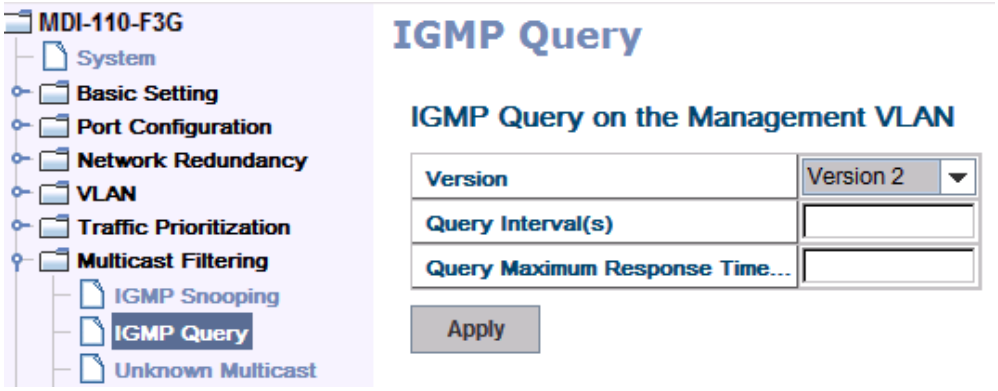
IGMP Snooping, you can select **Enable** or **Disable** here. After enabling IGMP Snooping, you can then enable IGMP Snooping for specific VLAN. You can enable IGMP Snooping for some VLANs so that some of the VLANs will support IGMP Snooping and others won't.

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: 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.

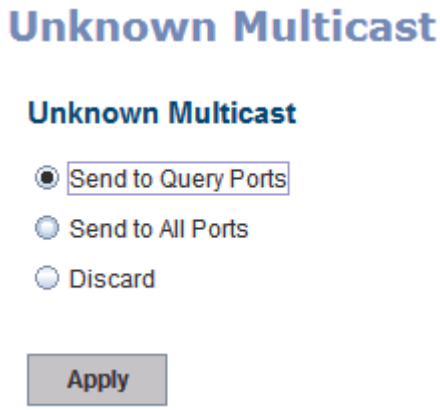
Query Interval(s): The period of query sent by querier.

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

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.



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.

4.8.4 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
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 1-2.
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 Vlan2 is IGMP snooping enabled Vlan3 is IGMP snooping disabled
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	
Unknown Multicast – Enable Force filtering (Send to All Ports) Disable Force filtering (Discard)	Switch(config)# mac-address-table multicast filtering Filtering unknown multicast addresses ok! Switch(config)# no mac-address-table multicast filtering Flooding unknown multicast addresses ok!
Unknown Multicast – Send to All Ports	Switch(config)# ip igmp snooping source-only-learning

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 series 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 section:

4.9.1 SNMP Configuration

4.9.2 SNMPv3 Profile

4.9.3 SNMP Traps

4.9.4 SNMP CLI Commands for SNMP

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.

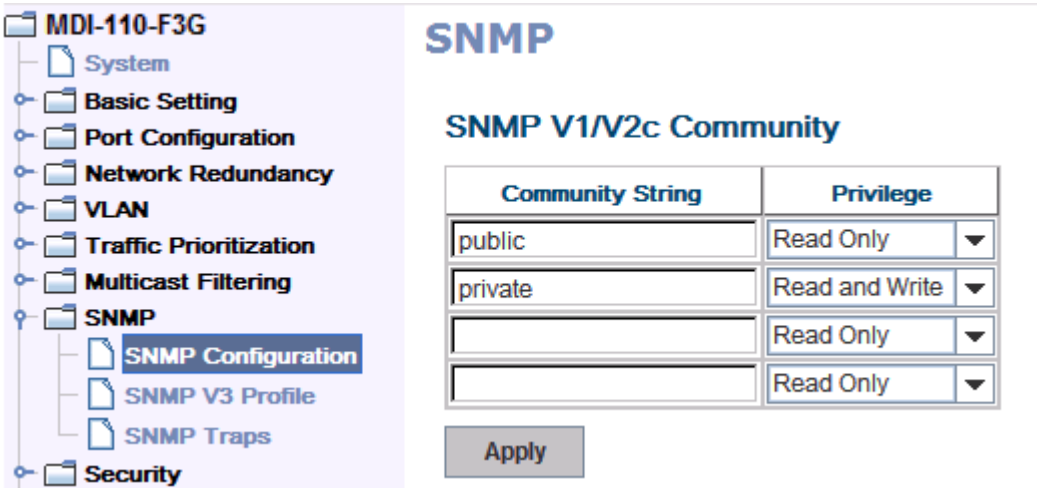
The community includes two privileges, Read Only and Read and Write.

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.

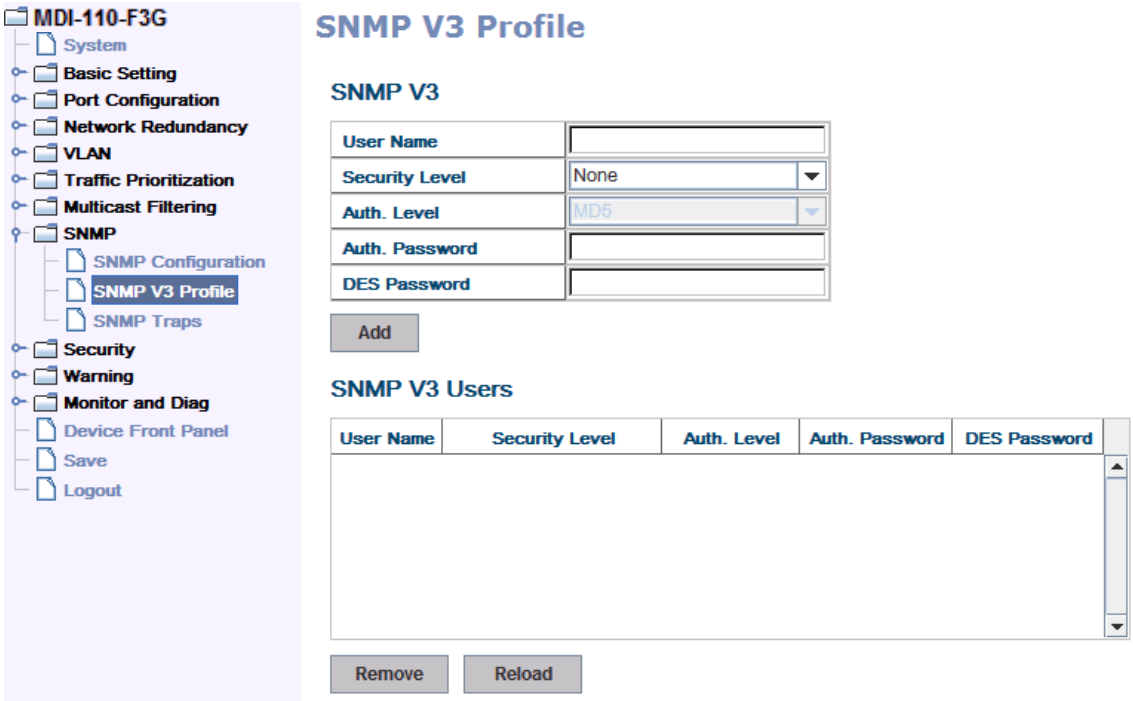
The switch allows users to assign four community strings. Type the community string and select the privilege. Then press **Apply**.

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.



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.



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.

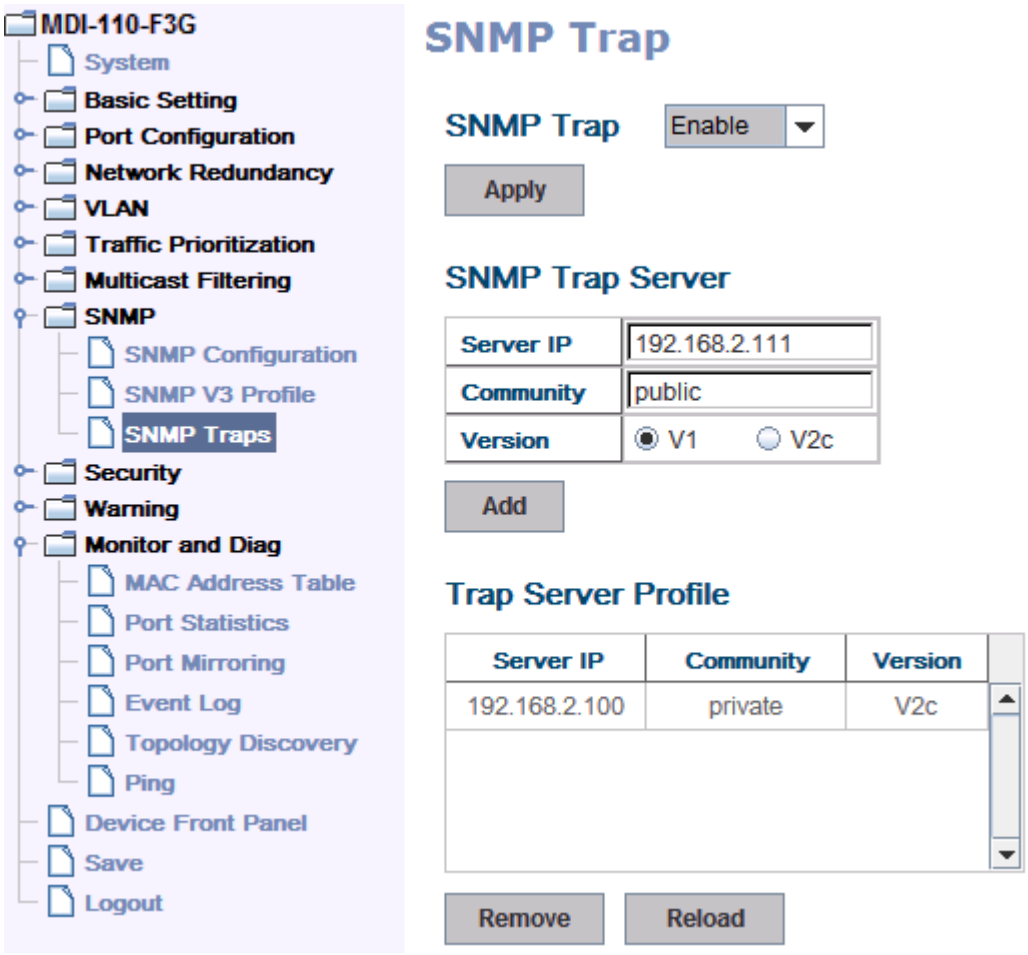
Authentication Password: Here the user enters the SNMP v3 user authentication password.

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.



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 features include Port Security and IP Security. Following commands are included in this section:

4.10.1 Port Security

4.10.2 IP Security

4.10.3 IEEE 802.1x

4.10.4 CLI Commands of the Security

4.10.1 Port Security

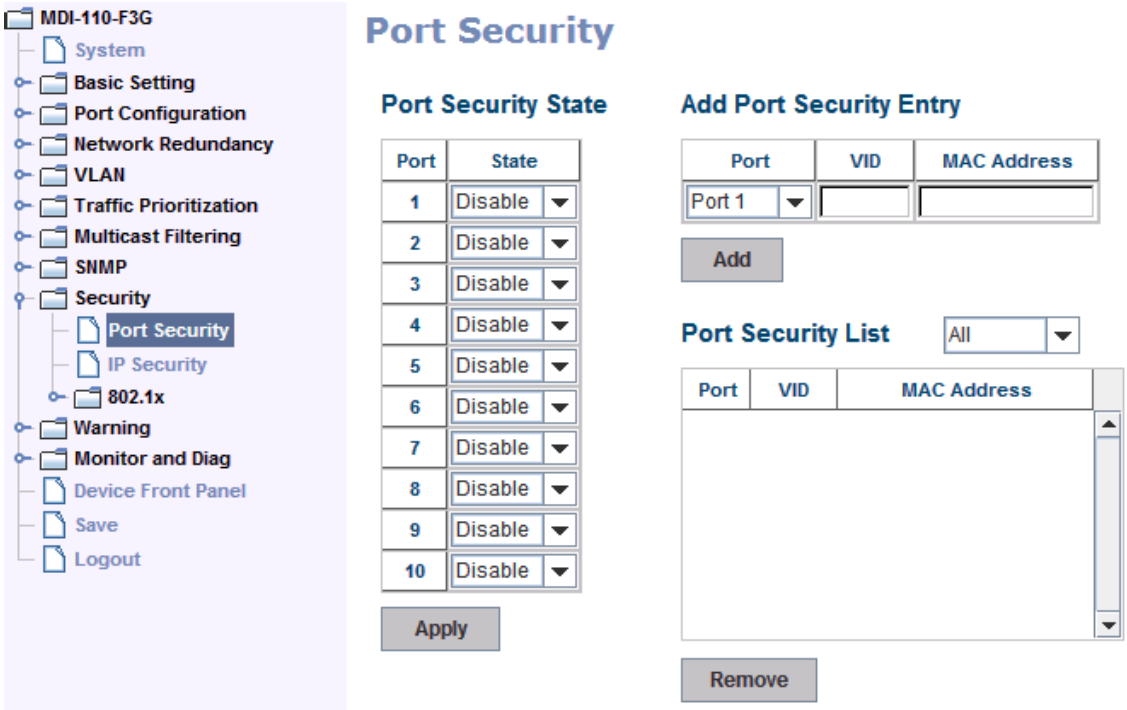
Port Security feature allows you to stop the MAC address learning for specific port. After stopping MAC learning, only the MAC address listed in Port Security List can access the switch and transmit/receive traffic. This is a simple way to secure your network - and can prevent to be accessed by hackers.

This page allows you to enable Port Security and configure Port Security entry.

Port Security State: Change Port Security State of the port to Enable first.

Add Port Security Entry: Select the port, and type VID and MAC address. Format of the MAC address is xxxx.xxxx.xxxx. Ex: 00:07:7c:e6:00:00. Max volume of one port is 10.and the switch can accept one hundred Port Security MAC addresses in total.

Port Security List: This table shows you those enabled port security entries. You can click on **Remove** to delete the entry.



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

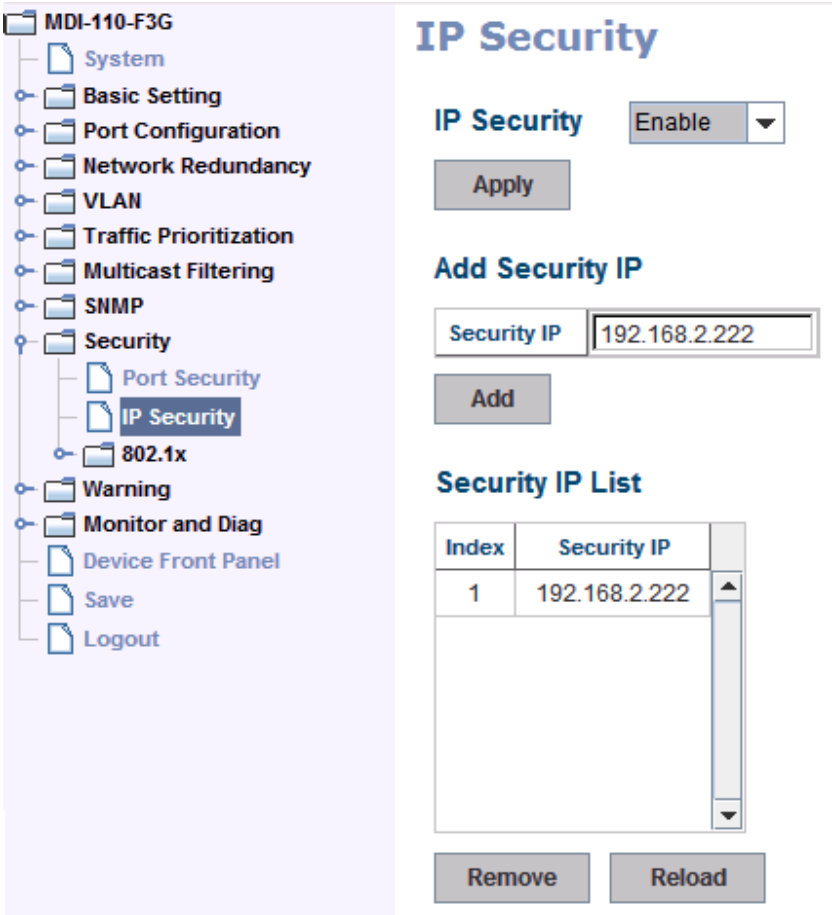
4.10.2 IP Security

In IP Security section, you can set up specific IP addresses to grant authorization for management access to this switch via a web browser or Telnet.

IP Security: Select Enable and **Apply** to enable IP security function.

Add Security IP: You can assign specific IP addresses, and then press **Add**. Only these IP addresses can access and manage switch via a web browser or Telnet. Maximum security IP address is ten.

Security IP List: This table shows you added security IP addresses. You can press **Remove** to delete, **Reload** to reload the table.

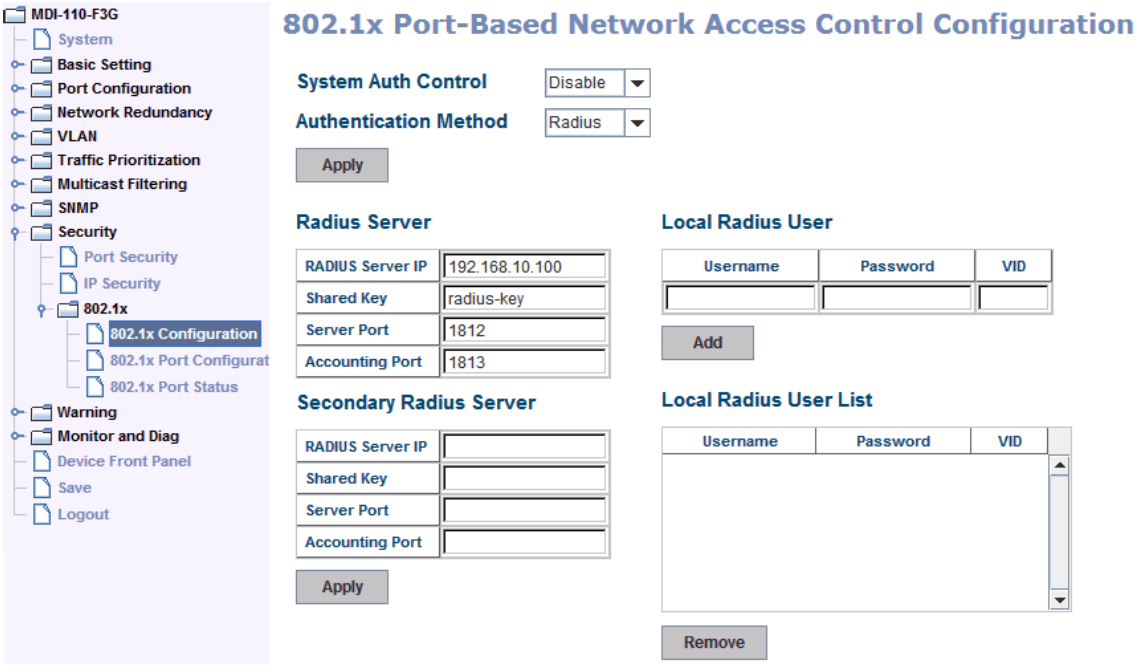


Once you finish configuring the settings, click on **Apply** to apply your configuration.

4.10.3 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.



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

Authentication Method: Radius is an authentication server that provides 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 create in this page for authentication.

Radius Server IP: The IP address of Radius server

Shared Key: The password between the switch and the 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: Backup Radius Server could be set in case of the primary radius server down.

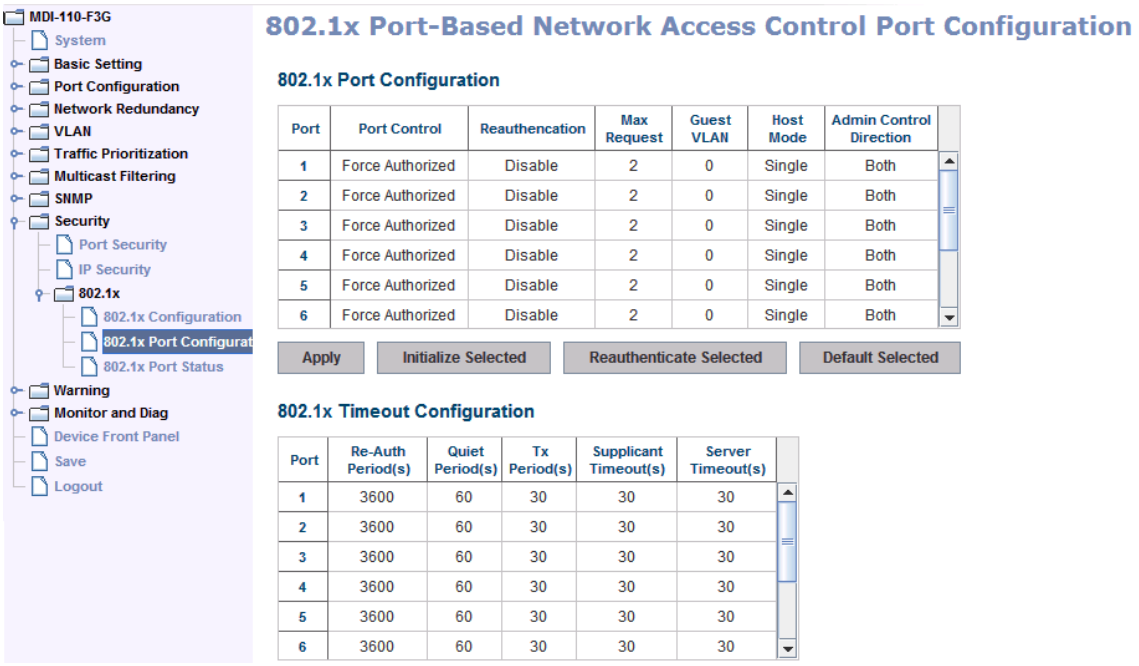
802.1X Local User: The User can add Account/Password for local authentication.

802.1X Local user List: This is a list shows the account information, User also can remove selected account Here.

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.



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 authentications. 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.

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

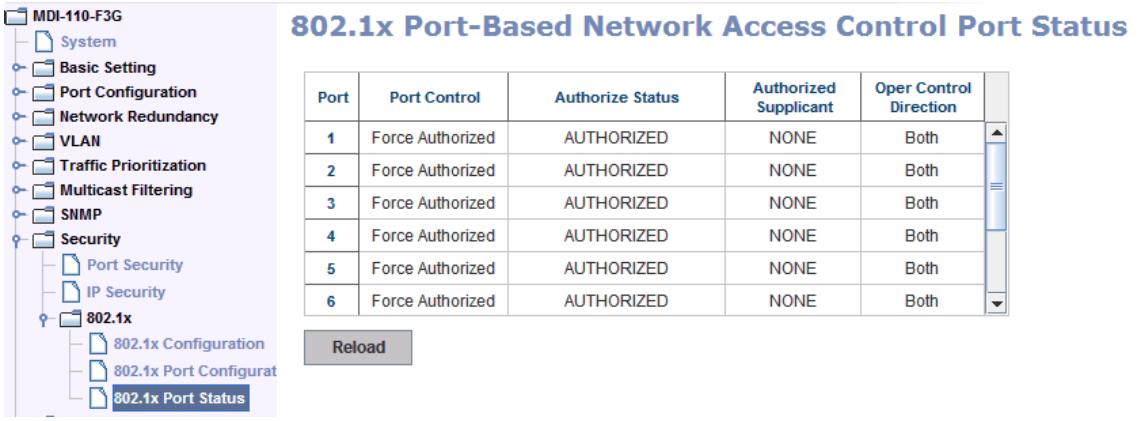
Click **Initialize Selected** to set the authorize state of selected port to initialize status.

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.



4.10.4 CLI Commands of the Security

Command Lines of the Security configuration

Feature	Command Line
Http / Telnet Security (only available for command line interface)	

Telnet service security	Switch# show service ; show current service status
	System service
	  Telnet : Enabled
	  Http : Enabled
	Switch(config)# service telnet ; it is recommended operating via local console interface only.
	  disable Disable telnet service ; stop service request from TCP port #23.
	  enable Enable telnet service; enable service request from TCP #23

	Switch(config)# service telnet enable Switch(config)# service telnet disable
Http service security	Switch(config)# service http; available operating via telnet or loca console interface. Switch(config)# service http disable ; diable TCP port #80 serivce. Switch(config)# service http enable; enable TCP port #80 serivce.
Port Security	
Add MAC	Switch(config)# mac-address-table static 0007.7c01.0101 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 ------------------- --------------- ------- ------------------------ 0007.7c01.0101 Static 1 fa1
IP Security	
IP Security	Switch(config)# ip security Set ip security enable ok. Switch(config)# ip security host 192.168.2.200 Add ip security host 192.168.2.200 ok.
Display	Switch# show ip security ip security is enabled ip security host: 192.168.2.200
802.1x	
enable	Switch(config)# dot1x system-auth-control Switch(config)#

diable	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

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 Fault Relay, System Log and SMTP E-mail Alert.

Following commands are included in this section:

4.11.1 Fault Relay

4.11.2 Event Selection

4.11.3 Syslog Configuration

4.11.4 SMTP Configuration

4.11.5 CLI Commands

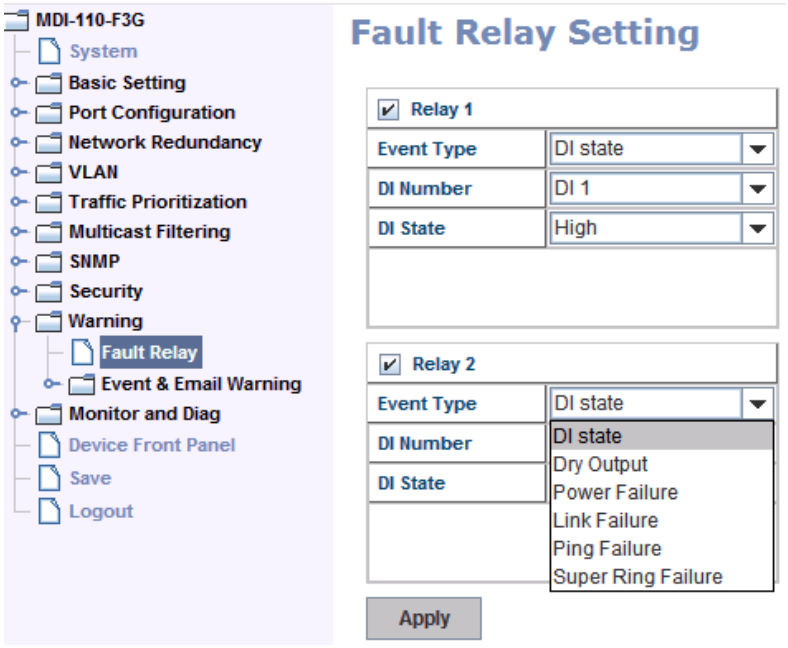
4.11.1 Fault Relay

The switch provides two digital outputs, also known as Relay Output. The relay contacts are energized (open) for normal operation and will close under fault conditions. Fault conditions include DI State change, Periodical On/Off, Power Failure, Ethernet port Link Failure, Ping Failure and Super Ring Topology Change. You can configure these settings in this Fault Relay Setting and each Relay can be assigned 1 fault condition.

Relay 1: Click on checkbox of the Relay 1, then select the Event Type and its parameters.

Relay 2: Click on checkbox of the Relay 2, then select the Event Type and its parameters.

Event Type: DI State, Dry Output, Power Failure, Link Failure, Ping Failure and Super Ring Failure. Each event type has its own parameters and should also be configured. Currently, each Relay can have one event type.



Event Type: **DI State**

DI Number: Select DI 1 or DI 2. Select which DI you want to monitor.

DI State: High or Low. Select the power voltage you want to monitor.

How to configure: Select the DI Number you want to monitor and DI State, High or Low. For example: When DI 1 and High are selected, it means when DI 1 is pulled high, the system will short Relay Output and light DO LED.

Event Type: **Dry Output**

On Period (Sec): Type the period time to turn on Relay Output. Available range of a period is 0-4294967295 seconds.

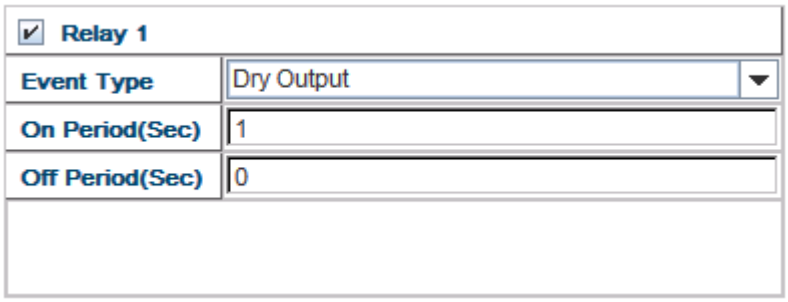
Off Period (Sec): Type the period time to turn off Relay Output. Available range of a period is 0-4294967295 seconds.

How to configure: Type turn-on period and turn-off period when the time is reached, the system will turn on or off the Relay Output. If you connect DO to DI of the other terminal unit, the setting can help you to change DI state. If you connect DO to the power set of other terminal units, this setting can help you to turn on or off the unit.

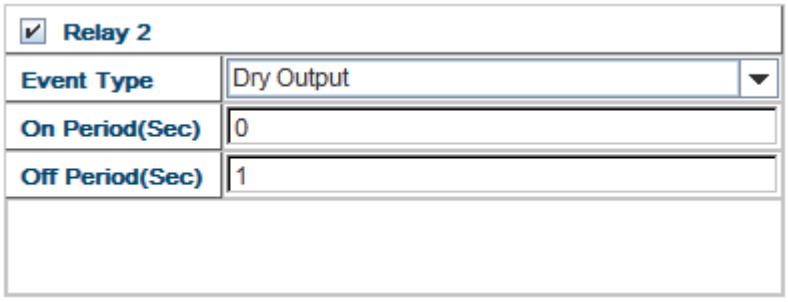
How to turn On/Off the other device: Type "1" into the "On period" field and "0" into "Off Period" field and apply the setting, then it t will be trigger to form as a close circuit.

To turn off the relay, just type "0" into the "On period" field and "1" into "Off Period" field and apply the setting, the relay will be trigger to form as an open circuit.

This function is also available in CLI, SNMP management interface. See the following setting.



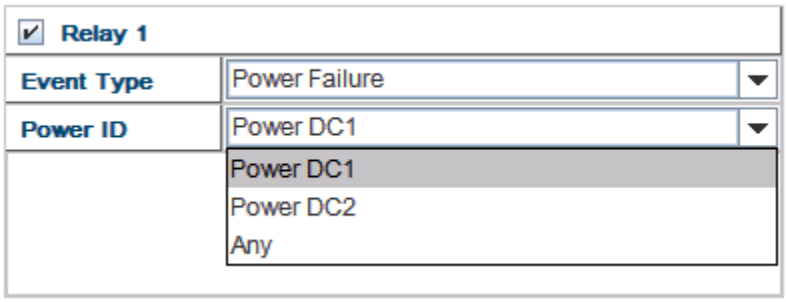
Turn on the relay output



Turn off the relay output

Event Type: **Power Failure**

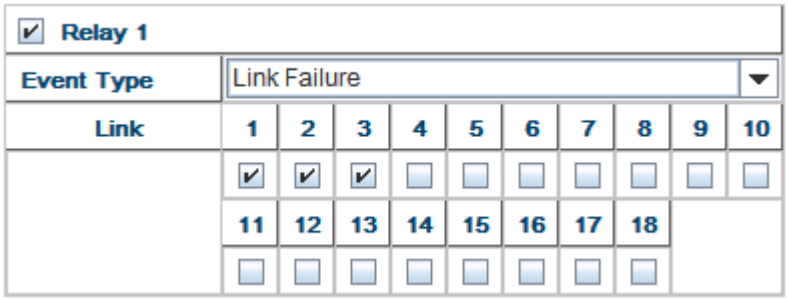
Power ID: Select Power 1 or Power 2 you want to monitor. When the power is shut down or broken, the system will short Relay Out and light the DO LED.



Event Type: **Like Failure**

Link: Select the port ID you want to monitor.

How to configure: Select the checkbox of the Ethernet ports you want to monitor. You can select one or multiple ports. When the selected ports are physically down, the system will short Relay Output and light the DO LED.

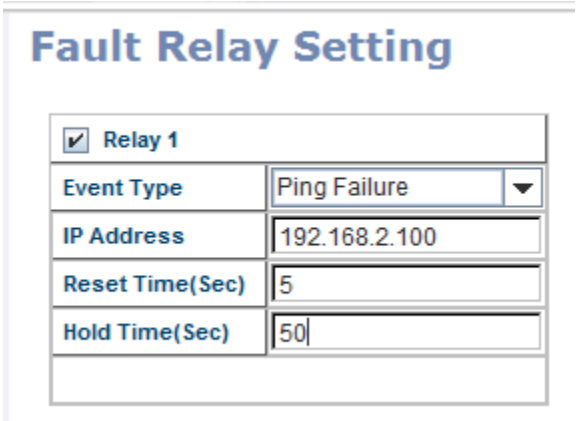


Event Type: **Ping Failure**

IP Address: IP address of the target device you want to ping.

Reset Time (Sec): Waiting time to short the relay output.

Hold Time (Sec): Waiting time to ping the target device for the duration of remote device boot



How to configure: After selecting Ping Failure event type, the system will turn Relay Output to short state and continuously ping the target device. When the ping failure occurred, the switch will turn the Relay Output to open state for a period of Reset Time.

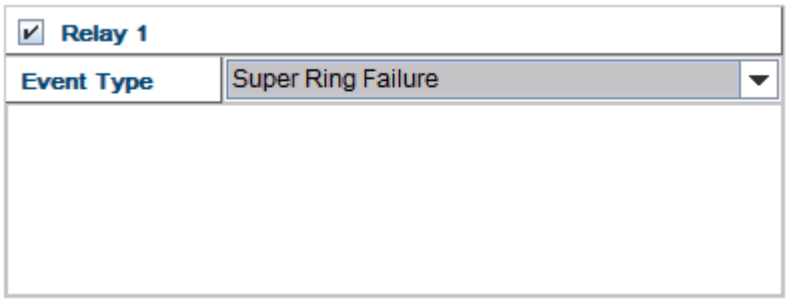
After the Reset Time timeout, the system will turn the Relay Output to close state. After the Hold Time timer is timeout, the switch system will start ping the target device.

Ex: Reset Time is 5 sec, Hold Time is 50 sec.

If the ping failure occurred, the switch system will turn Relay output to open state to emulate power switch off for 5 sec periods. After Reset Time timeout, the Switch system will start ping target device after 50 sec periods. The period time is for target device system booting. During the period, the switch system will not ping target device until Hold Time is timeout.

Event Type: **Super Ring Failure**

Select Super Ring Failure. When the Rapid Super Ring topology is changed, the system will short Relay Out and lengthen DO LED.

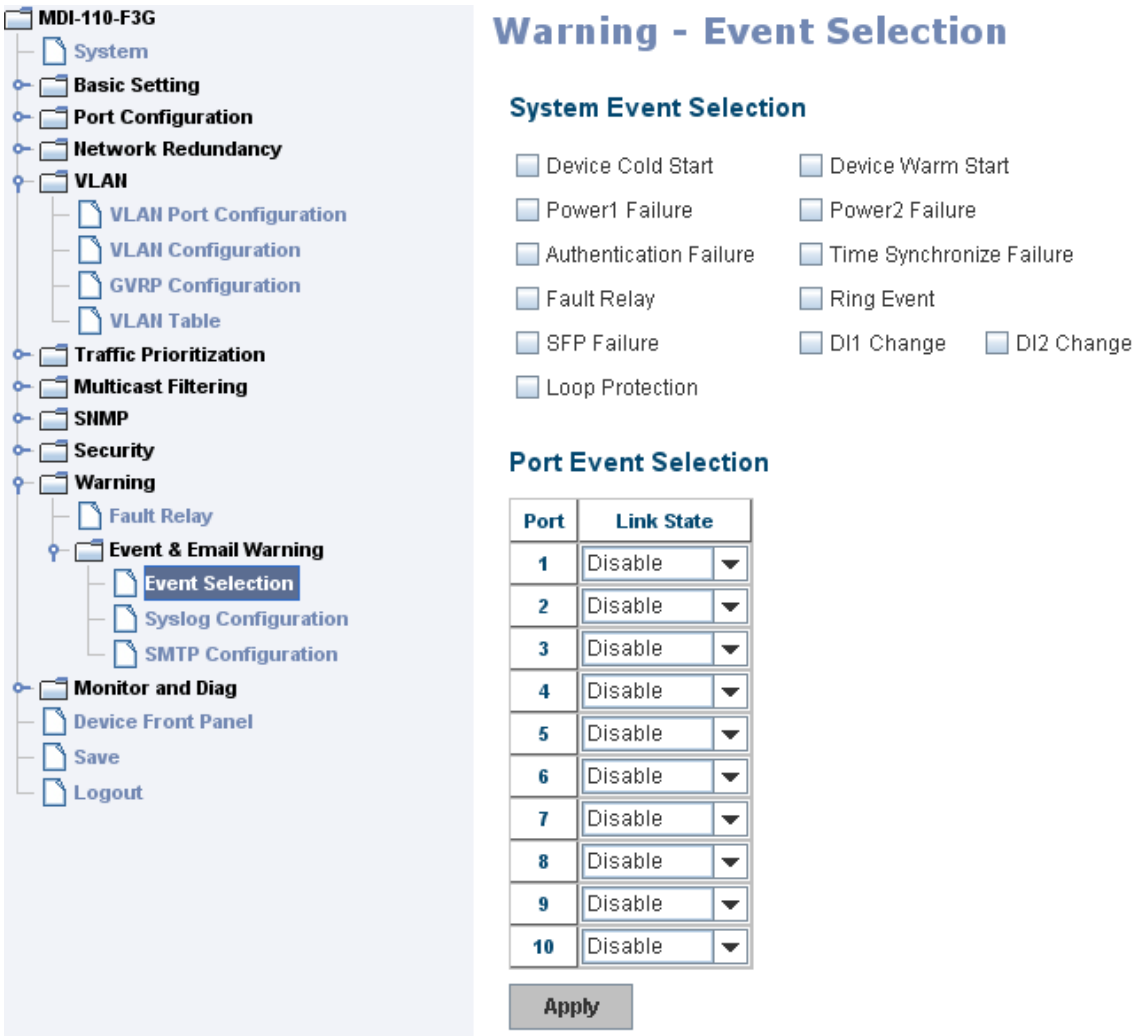


Once you finish configuring the settings, click on **Apply** to apply your configuration.

4.11.2 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 the 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.
Power 1 Failure	Power 1 is failure.
Power 2 Failure	Power 2 is failure.
Authentication failure	An incorrect password, SNMP Community String is entered.
Time Synchronize Failure	Accessing to NTP Server is failure.
Fault Relay	The DO/Fault Relay is on.
Ring Event	Master of Super Ring has changed or backup path is activated.
DI1 Change	The Digital Input#1 status is changed.
DI2 Change	The Digital Input#2 status is changed.
SFP DDM Failure	The readed information of DDM SFP transceiver is over temperature or out the range of TX/RX power.
Loop Protection	Port Looping is detected.
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)
Both	The link status changed.



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

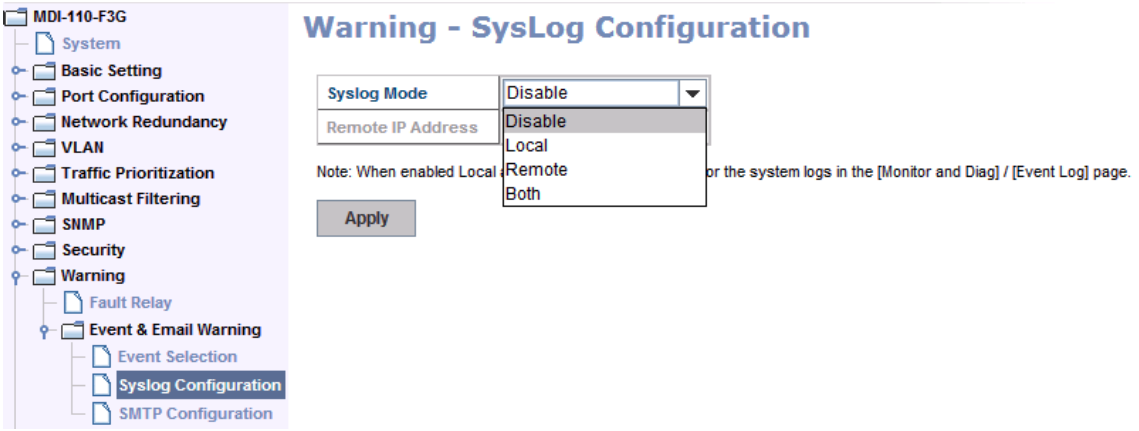
4.11.3 SysLog Configuration

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: 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.



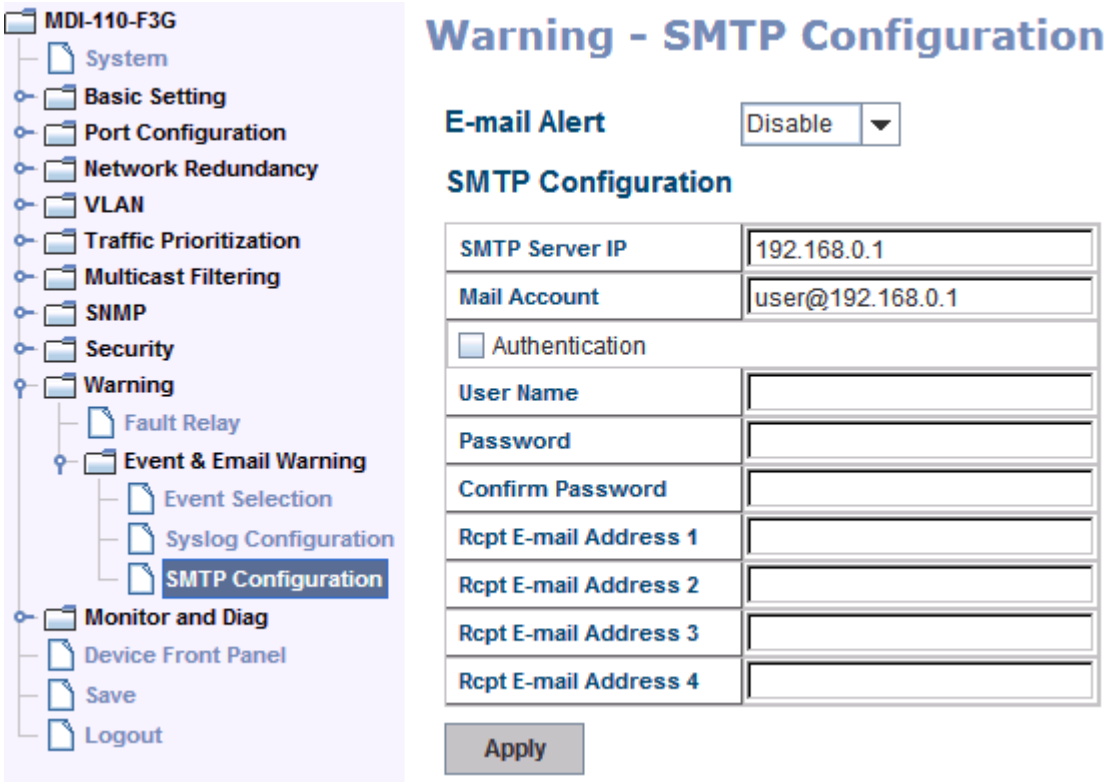
Once you finish configuring the settings, click on **Apply** to apply your configuration.

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

4.11.4 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.



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 the switch	
Rcpt E-mail Address 1	The first email address to receive email alert from the switch (Max. 40 characters)
Rcpt E-mail Address 2	The second email address to receive email alert from the switch (Max. 40 characters)
Rcpt E-mail Address 3	The third email address to receive email alert from the switch (Max. 40 characters)
Rcpt E-mail Address 4	The fourth email address to receive email alert from the switch (Max. 40 characters)

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

4.11.5 CLI Commands

Command Lines of the Warning configuration

Feature	Command Line
Relay Output	
Relay Output	Switch(config)# relay 1 di DI state dry dry output ping ping failure port port link failure power power failure ring super ring failure **Note: Select Relay 1 or 2 first, then select the event types.**
DI State	Switch(config)# relay 1 di <1-2> DI number Switch(config)# relay 1 di 1

	high high is abnormal low low is abnormal Switch(config)# relay 1 di 1 high
Dry Output	Switch(config)# relay 1 dry <0-4294967295> turn on period in second Switch(config)# relay 1 dry 5 <0-4294967295> turn off period in second Switch(config)# relay 1 dry 5 5
Ping Failure	Switch(config)# relay 1 ping 192.168.2.200 <cr> reset reset a device Switch(config)# relay 1 ping 192.168.2.200 reset <1-65535> reset time Switch(config)# relay 1 ping 192.168.2.200 reset 60 <0-65535> hold time to retry Switch(config)# relay 1 ping 192.168.2.200 reset 60 60
Port Link Failure	Switch(config)# relay 1 port PORTLIST port list Switch(config)# relay 1 port fa1-5
Power Failure	Switch(config)# relay 1 power <1-2> power id Switch(config)# relay 1 power 1 Switch(config)# relay 1 power 2
Super Ring Failure	Switch(config)# relay 1 ring
Disable Relay	Switch(config)# no relay <1-2> relay id Switch(config)# no relay 1 (Relay_ID: 1 or 2) <cr>
Display	Switch# show relay 1 Relay Output Type : Port Link Port : 1, 2, 3, 4, Switch# show relay 2 Relay Output Type : Super Ring
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 all Switch all event authentication Authentication failure event di Switch di event fault-relay Switch fault relay event loop-protect Switch loop protection event power Switch power failure event sfp-ddm Switch SFP DDM abnormal 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 Power Failure: Super Ring Topology Change: Disabled Fault Relay: Disabled Time synchronize Failure: Disable SFP DDM: Enabled DI:DI1
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: admin@Westermo.com ok.
Receiver mail	Switch(config)# smtp-server receipt 1 support@westermo.se SMTP Email Alert set receipt 1: support@westermo.com 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: 192.168.2.200, Account: support@Westermo.se 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 section:

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

4.12.5 Ping

4.12.6 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 and 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.

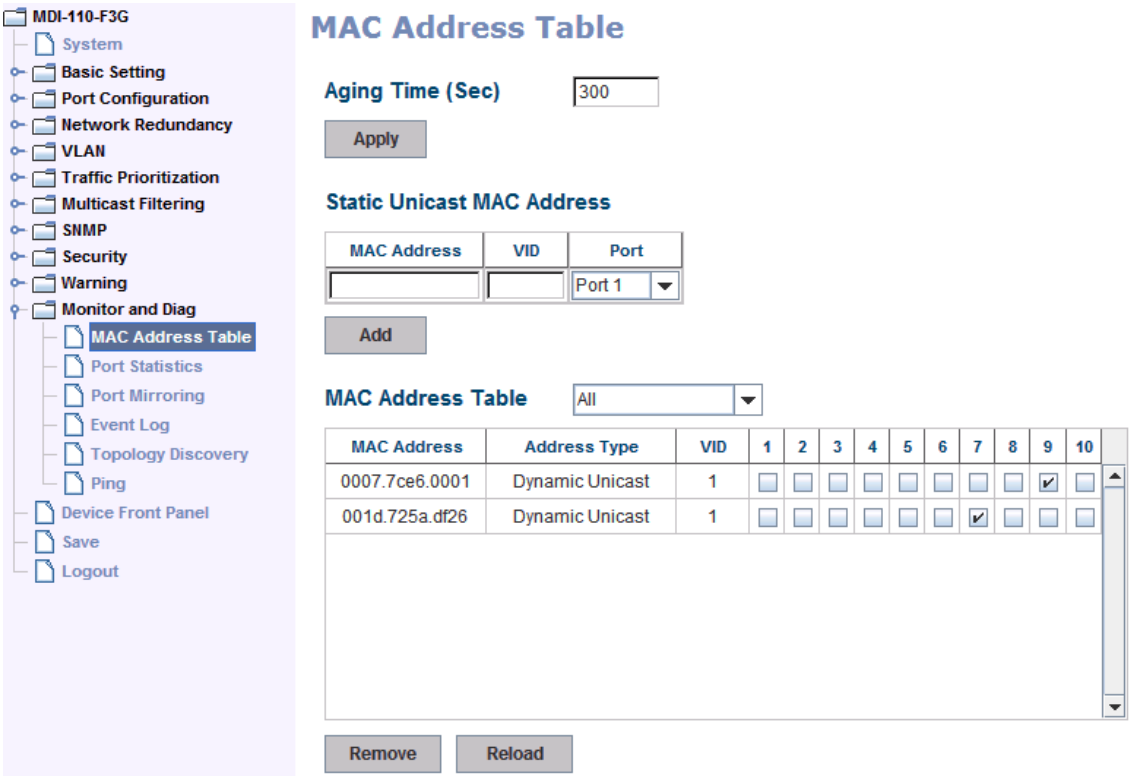
MAC Address Table

In this MAC Address Table, you can see all the MAC Addresses learned 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.

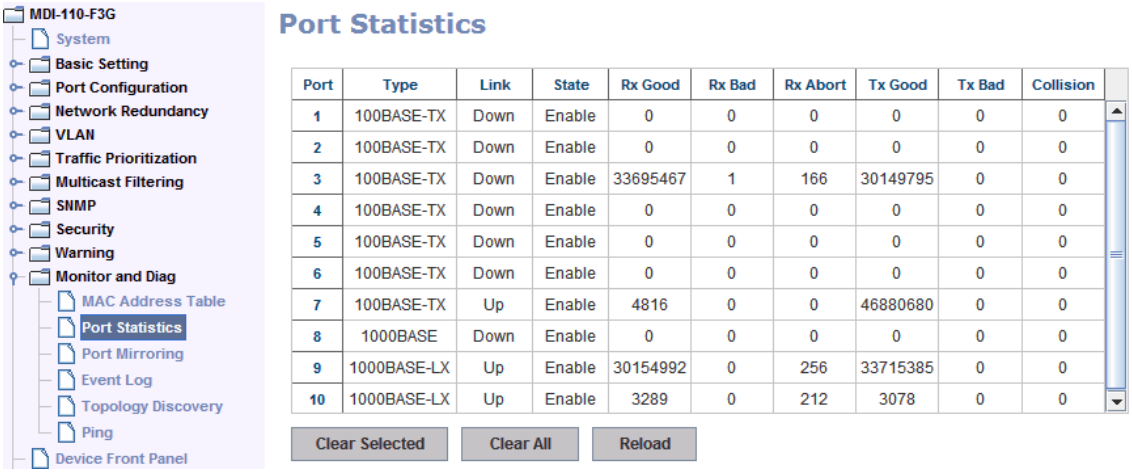


4.12.2 Port Statistics

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.



4.12.3 Port Mirroring

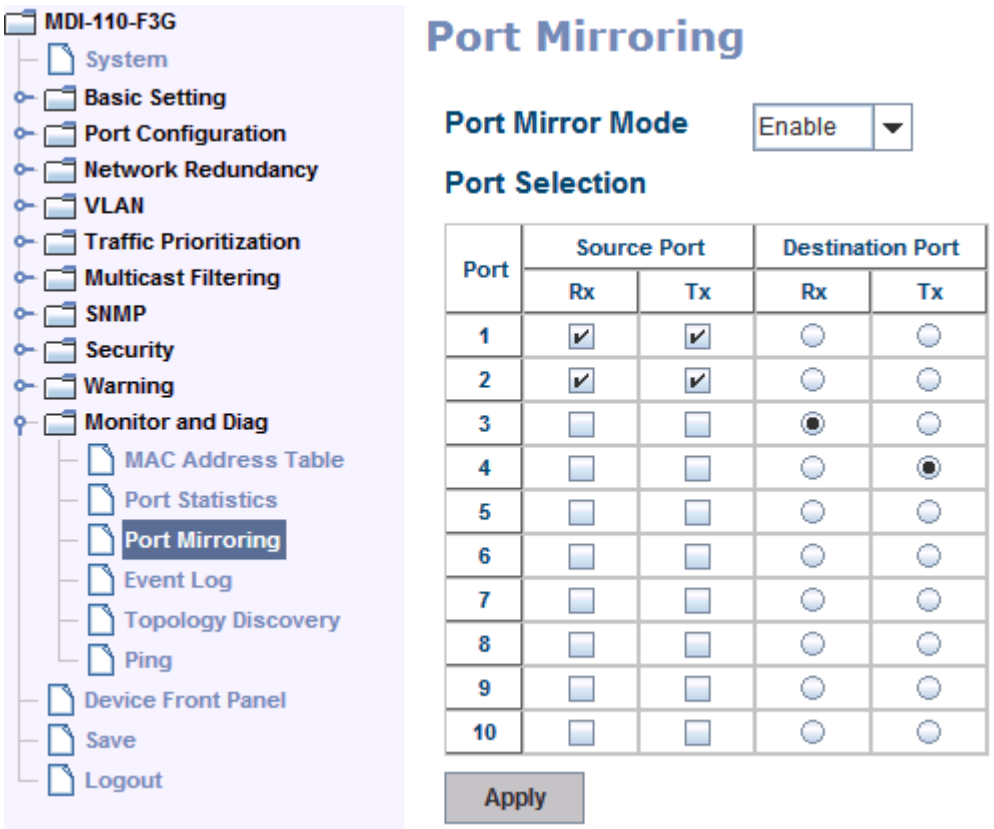
Port mirroring (also called port spanning) is a tool that allows you to mirror the traffic from one or more ports onto another port, without disrupting the flow of traffic on the original port. Any traffic that goes in or out of the Source Port(s) will be duplicated at the Destination Port. This traffic 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 a single port, or any combination of ports, but you can only monitor them in Rx or TX only. Click on checkbox of the Port ID, RX, Tx or Both 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 RX/TX of the destination port can be selected. A network administrator would typically connect a LAN analyzer to this port.

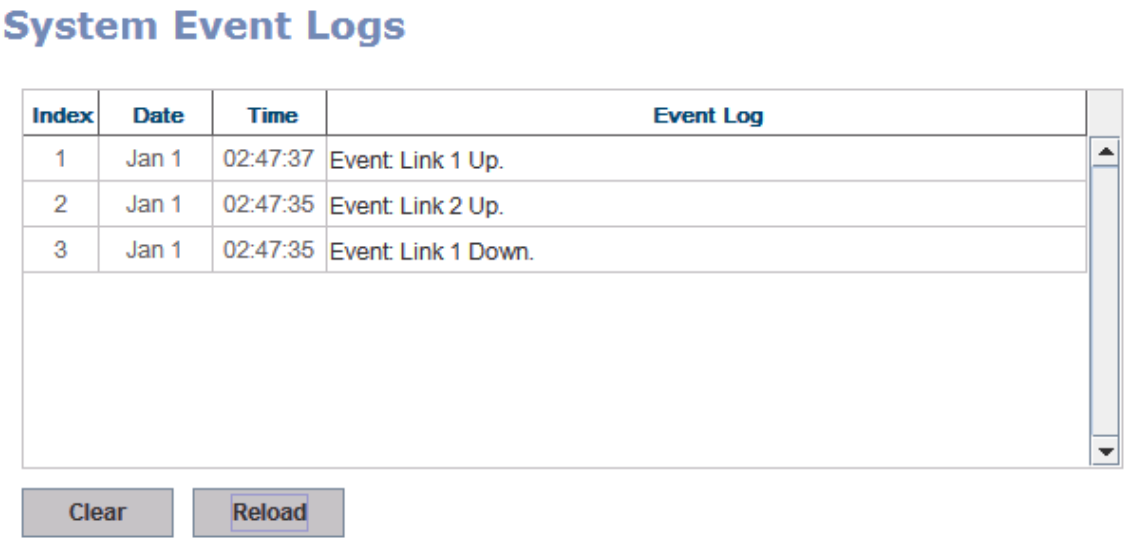
Once you finish configuring the settings, click on **Apply** to apply the settings.



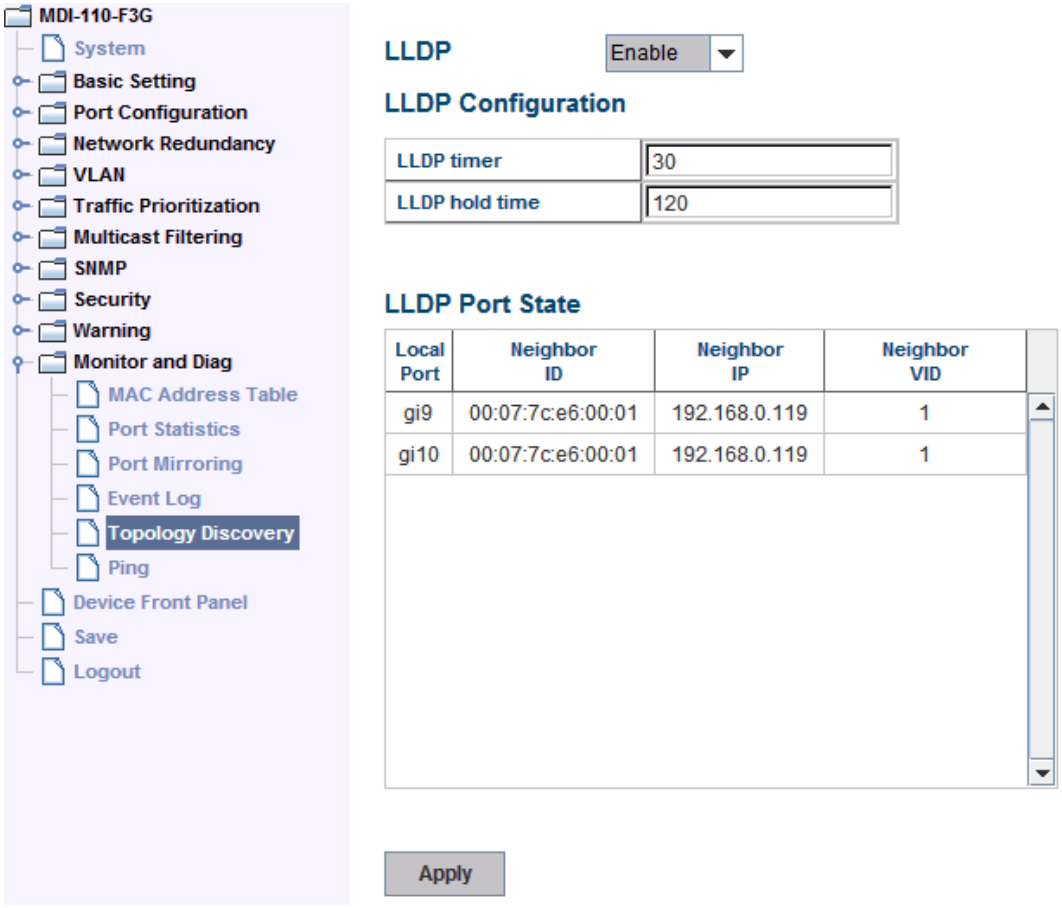
4.12.4 Event Log

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.



4.12.5 Topology Discovery



The switch supports topology discovery or LLDP (IEEE 802.1AB Link Layer Discovery Protocol) function that can help user to discovery multi-vendor's network device on same segment by NMS system which supports LLDP function; With LLDP function, 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: Select Enable/Disable to enable/disable LLDP function.

LLDP Configuration: To configure the related timer of LLDP.

LLDP Timer: The interval time of each LLDP and counts in second; the valid number is from 5 to 254, default is 30 seconds.

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

Local port: The current port number that linked with neighbor network device.

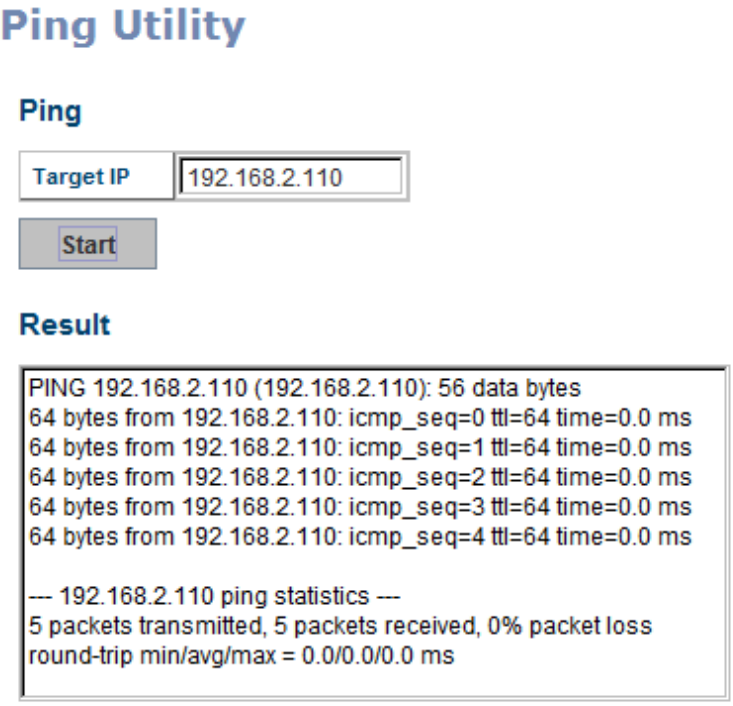
Neighbor ID: The MAC address of neighbor device on the same network segment.

Neighbor IP: The IP address of neighbor device on the same network segment.

Neighbor VID: The VLAN ID of neighbor device on the same network segment.

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.



4.12.7 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 0007.7c01.0101 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 000d.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 0007.7c01.0386 Dynamic 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.

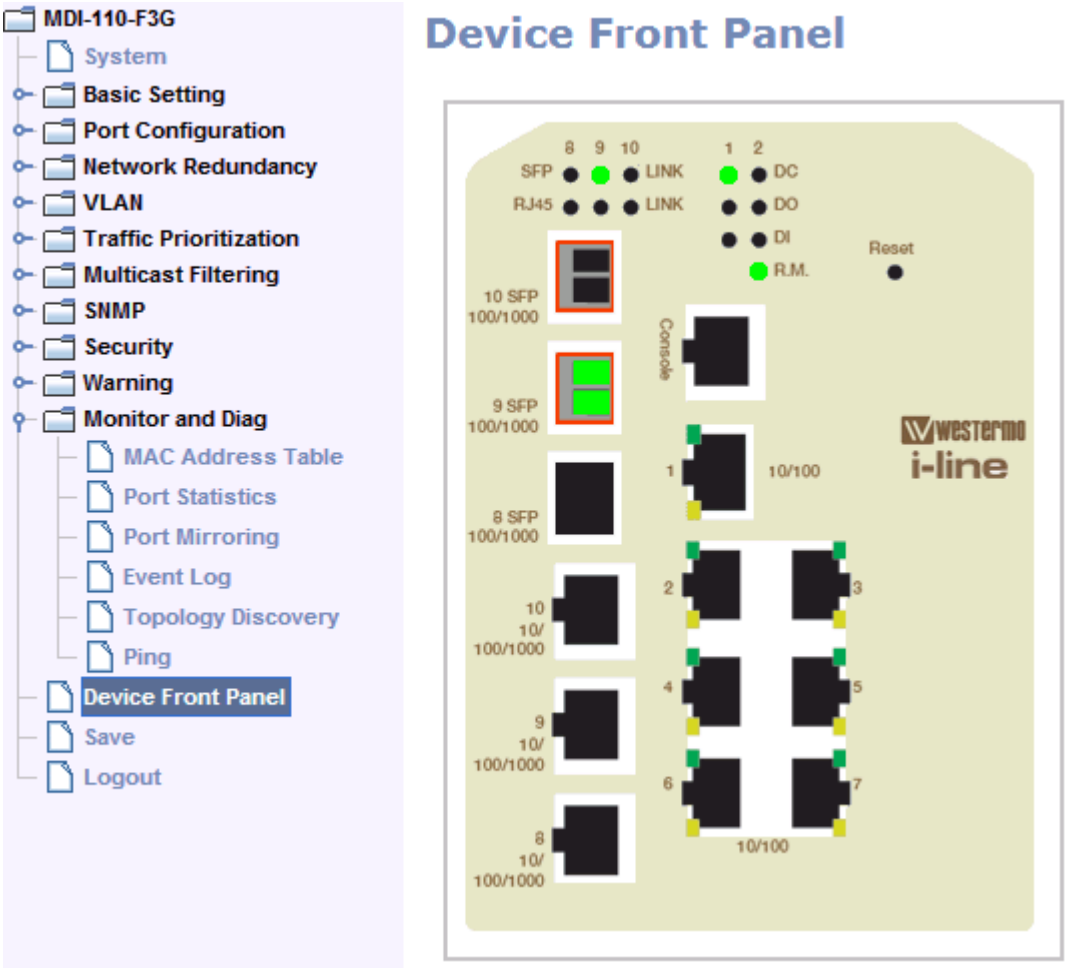
Select Source Port	Switch(config)# mirror source fa1-2 both Received and transmitted traffic rx Received traffic tx Transmitted traffic Switch(config)# mirror source fa1-2 both Mirror source fa1-2 both set ok. **Note: Select source port list and TX/RX/Both mode.**
Select Destination Port	Switch(config)# 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

4.12 Device Front Panel

Device Front Panel commands 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	Other
Power	Green	Black	
Digital Output	Green	Black	
Digital Input	Green	Black	
R.M.(Ring Master)	Green	Black	
Fast Ethernet	Green	Black	
Gigabit Ethernet	Green	Black	
SFP	Green	Black	Gray: Plugged but not link up yet.



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 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:

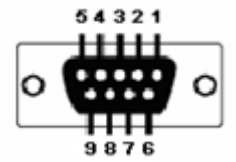
Feature	Command Line
Logout	SWITCH> exit SWITCH# exit

5 Appendix

5.1 Pin Assignment of the RS-232 Console Cable

The total cable length is 150cm, excluding RJ-45 and DB-9!

DB-9 is 'Female.'



RJ-45 Pin	DB-9 Pin	Description
1	8	N/A
2	9	N/A
3	**2**	**TxD**
4	1	N/A
5	**5**	**GND**
6	**3**	**RxD**
7	4	N/A
8	7	N/A

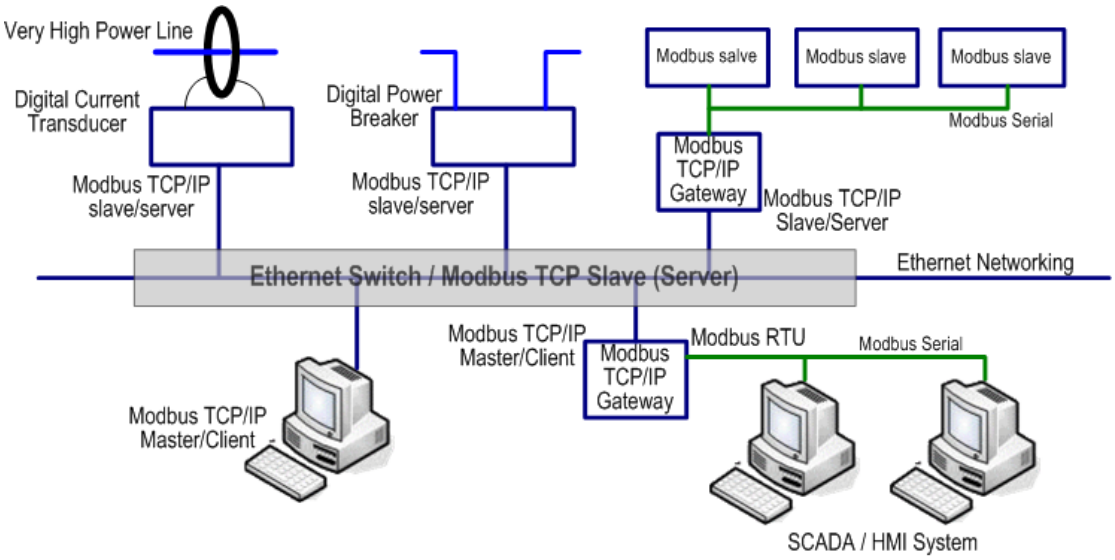
5.2 Private MIB

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 Modbus TCP /IP

The Modbus TCP/IP is very similar to Modbus RTU, but transmits data within TCP/IP Data packets. It was developed in 1979 for industrial automatic communication system and have becomes a standard protocol for industrial communication for the transfer discrete analogy I/O devices or PLC systems. It defines a simple protocol data unit independent of the underlying data link layer. The modbus TCP packet includes 3 parts - MBAP header, function code and data payload, the MBAP header is used on TCP/IP header to identify the Modbus application Data Unit and provides some differences compared to the MODBUS RTU application data unit used on serial line. The MBAP header also includes unit identifier to recognize and communicate between multiple independent modbus end units.

The modbus devices communicate using a master (client) /slave (server) architecture, only one device can initiate transaction and the others respond to the master/client. The other devices (slave/server) respond by supplying the requested data to the master/client, or by taking the action requested in the query. The slave/server can be any peripheral device (DSC unit, PLC unit, Volt/Current Transducer, network communication switch) which process information and sends the output data to the master using modbus TCP protocol. Westermo MDI-110 Switch operating as slave/server devices, while a typical master/client device is host computer running appropriate application software, like as SCADA / HMI system. The transaction architecture like as the drawing following.



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.

The MDI-110 Managed DIN-Rail Ethernet Switch has implement Modbus/TCP register in the firmware. Those register mapping to some of Ethernet Switchs' operating information, includes description, IP address, power status, interface status, interface information and inbound/outbound packet statistics. With the register supports, user can read the information through their own Modbus TCP based progress/ display/ monitor applications and monitor the status of the switch easily.

The configuration of Modbus/TCP only present in CLI management mode and the no extra user interface for Web configuration.

5.3.1 Modbus Function Code

The Modbus TCP device uses a subset of the standard Modbus TCP function code to access device-dependent information. Modbus TCP function code is defined as below.

FC	Name	Usage
01	Read Coils	Read the state of a digital output
02	Read Input Status	Read the state of a digital input
03	Read Holding Register	Read holding register in 16-bits register format

04	Read Input Registers	Read data in 16-bits register format
05	Write Coil	Write data to force a digital output ON/OFF
06	Write Single Register	Write data in 16-bits register format
15	Force Multiple Coils	Write data to force multiple consecutive coils

The MDI-110 device supports the function code 04, which name is Read Input Registers. With this support, the remove SCADA or other Modbus TCP application can poll the information of the device and monitor the major status of the switch.

5.3.2 Error Checking

The utilization of the error checking will help eliminate errors caused by noise in the communication link. In Modbus TCP mode, messages include an error-checking field that is based on a Cyclical Redundancy Check (CRC) method. The CRC filed checks the contents of the entire message. It applied regardless of any parity check method used for the individual BYTE actors of the message. The CRC value is calculated by the transmitting device, which appends the CRC to the message. The receiving device recalculates a CRC during receipt of the message, and compares the calculated value to the actual value it received in the CRC filed.

5.3.3 Exception Response

If an error occurs, the slave sends an exception response message to master consisting of the slave address, function code, exception response code and error check field. In an exception response, the slave sets the high-order bit (MSB) of the response function code to one. The exception response codes are listed below.

Code	Name	Descriptions
01	Illegal Function	The message function received is not allowable action.
02	Illegal Data Address	The address referenced in the data field is not valid.
03	Illegal Data Value	The value referenced at the addressed device location is no within range.
04	Slave Device Failure	An unrecoverable error occurred while the slave was attempting to perform the requested action.
05	Acknowledge	The slave has accepted the request and processing it, but a long duration of time will be required to do so.
06	Slave Device Busy	The slave is engaged in processing a long-duration program command.

07	Negative Acknowledge	The slave cannot perform the program function received in the query.
08	Memory Parity Error	The slave attempted to read extended memory, but detected a parity error in the memory.

5.3.4 Modbus TCP register table

The **7+3G** Switch and **7+3 100** Switch support Modbus TCP/IP client service for the Factory automation applications.

The command of modbus only supports in the command line interface- console and telnet mode that allows user to modify some parameters like as idle time, number of modbus master and modbus service port.

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 = "MDI-110-F3G" Word 0 Hi byte = ‘M’ Word 0 Lo byte = ‘D’ Word 1 Hi byte = ‘I’ Word 1 Lo byte = ‘-’ Word 2 Hi byte = ‘1’ Word 2 Lo byte = ‘1’ Word 3 Hi byte = ‘0’ Word 3 Lo byte = ‘-’ Word 4 Lo byte = ‘F’ Word 4 Hi byte = ‘3’ 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 = first number of version Word 0 Lo byte = second number of version Word 1 Hi byte = third number of version Word 1 Lo byte = extended character of version Ex: Version = v1.2a Word 0 Hi byte = 0x1 Word 0 Lo byte = 0x2 Word 1 Hi byte = 0x0 Word 1 Lo byte = 'a' Version = v1.2.3a Word 0 Hi byte = 0x1 Word 0 Lo byte = 0x2 Word 1 Hi byte = 0x3 Word 1 Lo byte = 'a' Version = v1.2.3.4 Word 0 Hi byte = 0x1 Word 0 Lo byte = 0x2 Word 1 Hi byte = 0x3 Word 1 Lo byte = 0x0
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 0x3FF	248 words	Reserved address space (IPv6 or others)
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 / RS (Green light) 0x0000:Off 0x0001:On
0x0422	1 word	RF / RS – (Yellow light) 0x0000:Off 0x0001:On
0x0423 to 0x0BFF	2103 words	Reserved address space
0x0C00	1 words	Clear all rmon information Write 0x0001 to clear Read to return 0x0000
0x0C01	1 words	Clear rmon by bitmap of port 1 to 16 Write to clear Read to return 0x0000 To clear port 1 Word = 0x0001 To clear port 1 and 2 Word = 0x0003
0x0C02	1 words	Clear rmon by bitmap of port 17 to 32 Write to clear Read to return 0x0000 To clear port 17 Word = 0x0001 To clear port 17 and 18 Word = 0x0003
0x0C03 to 0x0FFF	1021 words	Reserved address space
Port Information (32 Ports)		
0x1000 to 0x11FF	16 words	Port Name
0x1200 to	1 word	Administrative Status

0x121F		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	1 word	Default CoS Value for untagged packets

0x139F		
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 0x13FF	1 word	Medium type 0x0000: none 0x0001: 100baseTX 0x0002: 1000baseT 0x0003: 100BaseFX 0x0004: 1000BaseSX 0x0005: 1000BaseLX 0x0006: other fiber transceiver 0x0007: fiber transceiver is not present 0xFFFF: unavailable
0x1400 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 Raw data
0x1820 to 0x185F	2 words	Alarm Temperature Word 0 : Raw data of High Alarm Word 1 : Raw data of Low Alarm
0x1860 to 0x187F	1 words	Tx power Raw data
0x1880 to 0x18BF	2 words	Warning Tx power Word 0 : Raw data of High Alarm Word 1 : Raw data of Low Alarm
0x18C0 to 0x18DF	1 words	Rx power Raw data
0x18E0 to 0x191F	2 words	Warning Rx power Word 0 : Raw data of High Alarm Word 1 : Raw data of Low Alarm
0x1920 to 0x1FFF	1760 words	Reserved address space
Inbound packet information		
0x2000 to 0x203F	2 words	Good Octets
0x2040 to 0x207F	2 words	Bad Octets

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	Disacrds
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	192 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	2 words	Filtered

0x27FF		
0x2800 to 0x283F	2 words	FCSError
0x2840 to 0x29FF	448 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
0x2B80 to 0x2FFF	1152 words	Reserved address space
Network Redundancy Information		
0x3000	10 words	Ring 0's Name Ring Name = "Ring0" Word 0 Hi byte = 'R' Word 0 Lo byte = 'i' Word 1 Hi byte = 'n' Word 1 Lo byte = 'g' Word 2 Hi byte = '0' Word 2 Lo byte = '\0' (other words = 0)
0x300A	1 word	Ring 0's Status 0x0000: none 0x0001: disable 0x0002: normal 0x0003: abnormal
0x300B	1 word	Ring 0's Version 0x0000: none 0x0001: Super Ring 0x0002: Rapid Super Ring 0x0003: Any Ring 0x0004: not support 0xFFFF: unavailable
0x300C	1 word	Ring 0's Device Role 0x0000: none 0x0001: disable 0x0002: RM (Ring Master) 0x0003: non-RM 0xFFFF: unavailable
0x300D	2 word	Ring 0's Port List of 1st Ring Port Word 0 = port 1-16 Word 1 = port 17-32 Ex: 0x0001: Ethernet port 1 0x0002: Ethernet port 2 0x0003: Ethernet port 1 and 2
0x300F	2 word	Ring 0's Port List of 2nd Ring Port Word 0 = port 1-16

		Word 1 = port 17-32 Ex: 0x0001: Ethernet port 1 0x0002: Ethernet port 2 0x0003: Ethernet port 1 and 2
0x3011	3 words	Ring 0's Master 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
0x3014	2 word	Ring 0's Blocked Port List Word 0 = port 1-16 Word 1 = port 17-32 Ex: 0x0001: Ethernet port 1 0x0002: Ethernet port 2 0x0003: Ethernet port 1 and 2
0x3016	1 word	Ring 0's Rapid Dual Homing Status 0x0000: none 0x0001: disable 0x0002: enable 0xFFFF: unavailable
0x3017 to 0x301F	9 words	Reserved address space
0x3020 to 0x303F		Ring 1's Information
0x3040 to 0x305F		Ring 2's Information
0x3060 to 0x307F		Ring 3's Information
0x3080 to 0x309F		Ring 4's Information
0x30A0 to 0x30BF		Ring 5's Information
0x30C0 to 0x30DF		Ring 6's Information
0x30E0 to 0x30FF		Ring 7's Information
0x3100 to 0x311F		Ring 8's Information
0x3120 to 0x313F		Ring 9's Information
0x3140 to 0x315F		Ring 10's Information
0x3160 to 0x317F		Ring 11's Information
0x3180 to 0x319F		Ring 12's Information
0x31A0 to 0x31BF		Ring 13's Information
0x31C0 to 0x31DF		Ring 14's Information
0x31E0 to 0x31FF		Ring 15's Information

0x3200 to 0x321F		Ring 16's Information
0x3220 to 0x323F		Ring 17's Information
0x3240 to 0x325F		Ring 18's Information
0x3260 to 0x327F		Ring 19's Information
0x3280 to 0x329F		Ring 20's Information
0x32A0 to 0x32BF		Ring 21's Information
0x32C0 to 0x32DF		Ring 22's Information
0x32E0 to 0x32FF		Ring 23's Information
0x3300 to 0x331F		Ring 24's Information
0x3320 to 0x333F		Ring 25's Information
0x3340 to 0x335F		Ring 26's Information
0x3360 to 0x337F		Ring 27's Information
0x3380 to 0x339F		Ring 28's Information
0x33A0 to 0x33BF		Ring 29's Information
0x33C0 to 0x33DF		Ring 30's Information
0x33E0 to 0x33FF		Ring 31's Information

Note: the modbus TCP client will return 0xFFFF to modbus master when pulling reserved address.

5.3.5 CLI commands for Modbus TCP

The CLI commands of Modbus TCP are listed as following table.

Feature	Command & example
Enable Modbus TCP	Switch(config)# modbus enable
Disable Modbus TCP	Switch(config)# modbus disable
Set Modbus interval time between request	Switch(config)# modbus idle-timeout <200-10000> Timeout vlaue: 200-10000ms Switch(config)# modbus idle-timeout 200 → set interval request time out duration to 200ms.
Set modbus TCP master communicate session.	Switch(config)# modbus master <1-20> Max Modbus TCP Master Switch(config)# modbus master 2 → set maximum

	modbus master up to 2; maximum support up to 20 modbus communicate sessions.
Set modbus TCP listening port	Switch(config)# modbus port port Listening Port Switch(config)# modbus port 502 ; default modbus TCP service port is 502.

5.4 Revision History

Edition	Date	Modifications
V1.1	2013/10/22	Add new features to Modbus TCP protocol IPv6 features ■ new sfp functions: 1. Add eject/scan function 2. Add enable/disable DDM function 3. Add new warning event ■ Add Private VLAN and QinQ function ■ Power input range 10.5~60VDC, typical input DC24V in HW version V2.3. ■ Add loop protection function in network redundancy ■ Update daylight saving time picture for new time setting format ■ Add MSTP in Network Redundancy chapter. ■ Update STP function in Network Redundant chapter.
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.