

MDI-110 Series

User's Manual

Industrial Managed Ethernet Switch

Copyright Notice

Copyright © 2010 Westermo Technology Co., Ltd.

All rights reserved.

Reproduction in any form or by any means without permission is prohibited.

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	6
1.1	Overview	6
1.2	Major Features	7
1.3	Package List	7
2	Hardware Installation.....	8
2.1	Hardware Introduction	8
2.2	Wiring Power Inputs	9
2.3	Wiring Digital Input.....	10
2.4	Wiring Digital Output.....	11
2.5	Wiring Earth Ground.....	11
2.6	Wiring Fast Ethernet Ports.....	12
2.7	Wiring Combo Ports.....	13
2.8	Wiring RS-232 Console Cable.....	13
2.9	DIN-Rail Mounting Installation.....	13
2.10	Wall-Mounting Installation	15
2.11	Safety Warning.....	16
3	Preparation for Management	17
3.1	Preparation for Serial Console	17
3.2	Preparation for Web Interface	18
3.3	Preparation for Telnet Console	20
4	Feature Configuration	23
4.1	Command Line Interface Introduction.....	24
4.2	Basic Setting	29
4.3	Port Configuration.....	46
4.4	Network Redundancy.....	56
4.5	VLAN.....	67
4.6	Traffic Prioritization.....	77
4.7	Multicast Filtering	84
4.8	SNMP.....	90
4.9	Security	94
4.10	Warning.....	101
4.11	Monitor and Diag	112
4.12	Device Front Panel	122
4.13	Save to Flash.....	123
4.14	Logout	124

5	Appendix	125
5.1	Pin Assignment of the RS-232 Console Cable	125
5.2	Private MIB.....	126
5.3	Revision History.....	127

1 Introduction

Welcome to Westermo MDI-110 Series Industrial Managed Ethernet Switch User Manual. Following topics are covered in this chapter:

1.1 Overview

1.2 Major Features

1.3 Package Checklist

1.1 Overview

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, JetView 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 by 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. The fastest failover time is enhanced from 300ms to 5ms for 10/100TX RJ-45 ports, and 30ms for 100FX and Gigabit Fiber. 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 with Westermo switch or other managed switches.

The IP31-design 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. MDI-110 Series will be your best option for highly-managed industrial network.

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)
- 32G switch Fabric, 8K MAC address
- Patented Multiple Super Ring (MSR), minimum Recovery time <5ms
- Rapid Dual Homing, which allows switch connect to third party network with maximum 7 multiple redundant paths.
- Embedded Hardware Watchdog timer to auto reset when failure
- LACP/VLAN/GVRP/QoS/IGMP Snooping/IGMP Query/Rate Control/ Online Multi-Port Mirroring
- Secured by IEEE 802.1x, Port Security, Access IP list, SSH and HTTPS Login
- Event Notification by E-mail, SNMP trap and SysLog
- Cisco-Like CLI, Web, SNMP/RMON, and JetView for network Management
- Redundant DC Power Inputs, Digital Input and Relay Output
- 1.5KV Hi-Pot Protection for ports and power
- 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 in 6 mm length)
- 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

Panel Layout

Bottom View

2.2 Wiring Power Inputs

2.3 Wiring Digital Input

2.4 Wiring Relay Output

2.5 Wiring Ethernet Ports

2.6 Wiring Combo Ports

2.7 Wiring RS-232 console cable

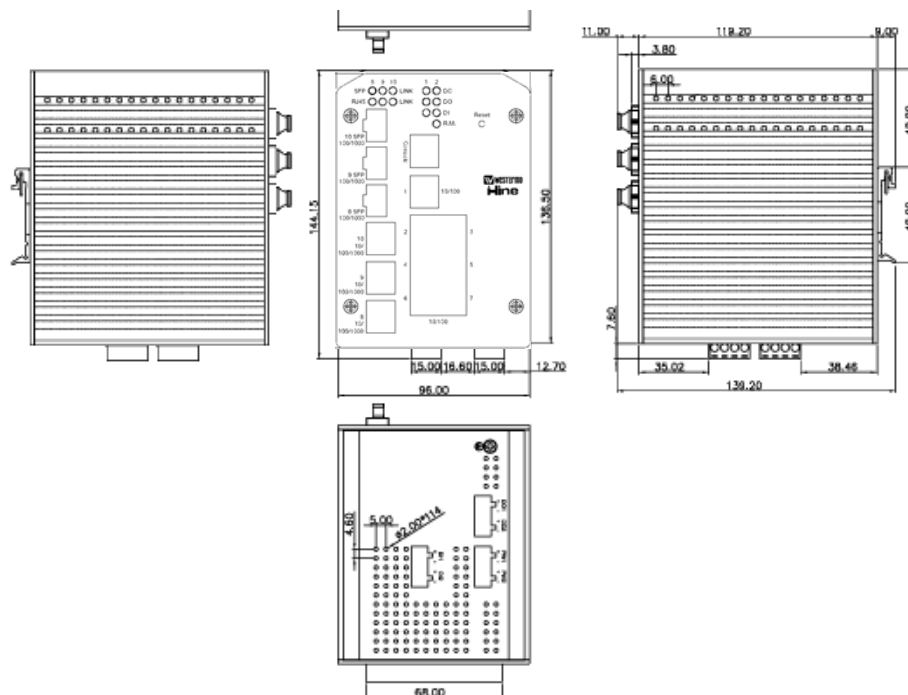
2.8 DIN-Rail Mounting Installation

2.9 Wall-Mounting Installation

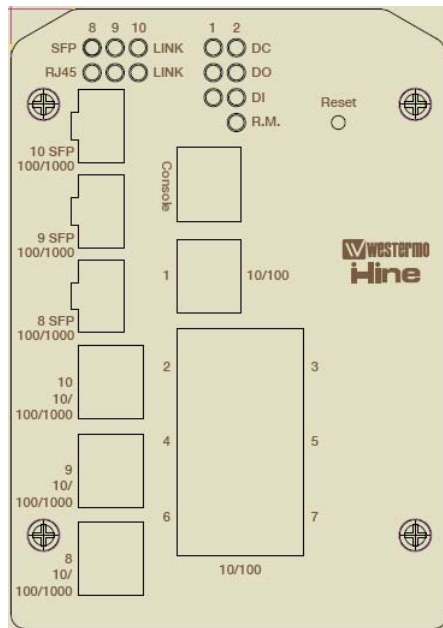
2.1 Hardware Introduction

Dimension

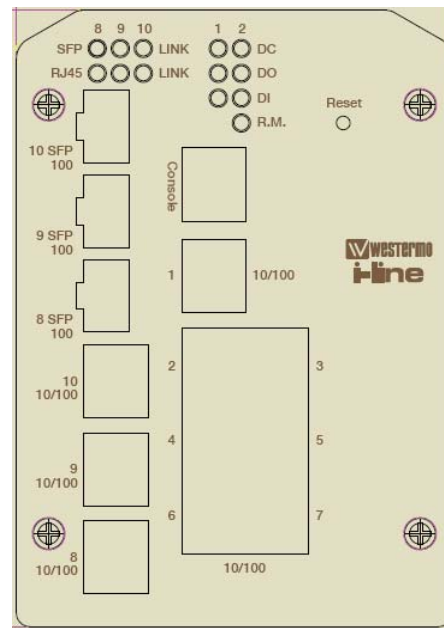
The switch dimension (W x H x D) is **96mm x 137mm x 119mm**



Panel Layout



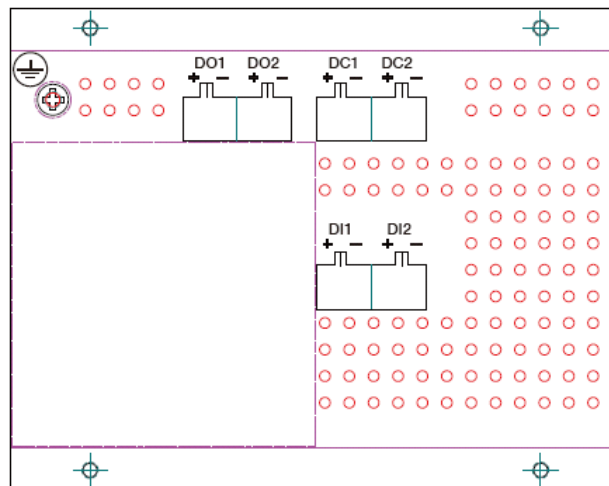
MDI-110-F3G



MDI-110-F3

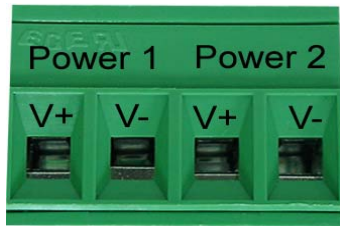
Bottom View

The bottom view of the switch consists of three terminal block connectors with two DC power inputs, two Digital Inputs, 2 Relay Outputs and 1 Earth Ground.

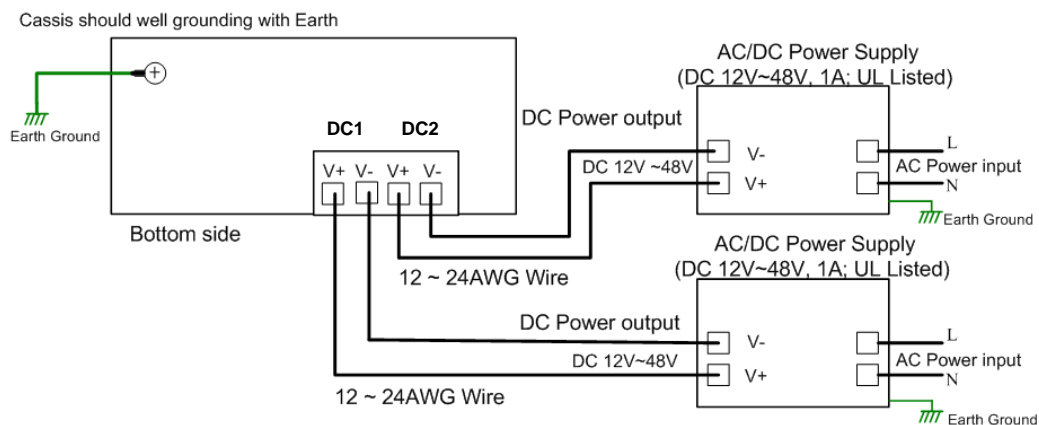


2.2 Wiring Power Inputs

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 PWR1 or PWR2.
- Note 4:** To use the UL Listed Power supply with output Rating 12-48 Vdc, minimum 1 A

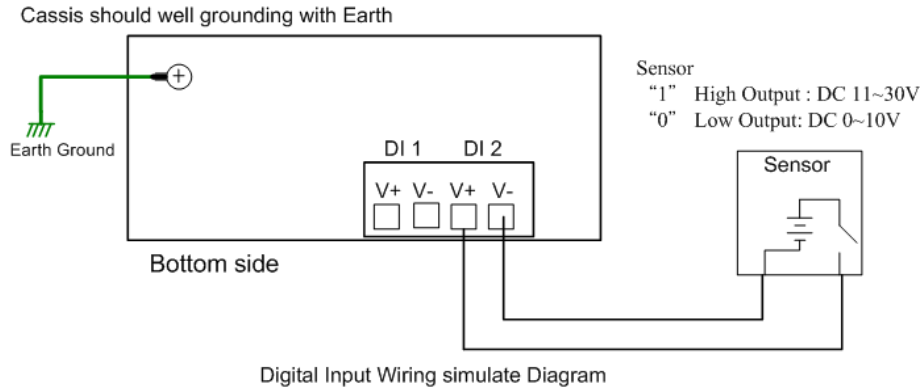
2.3 Wiring Digital Input

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 equipments 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.

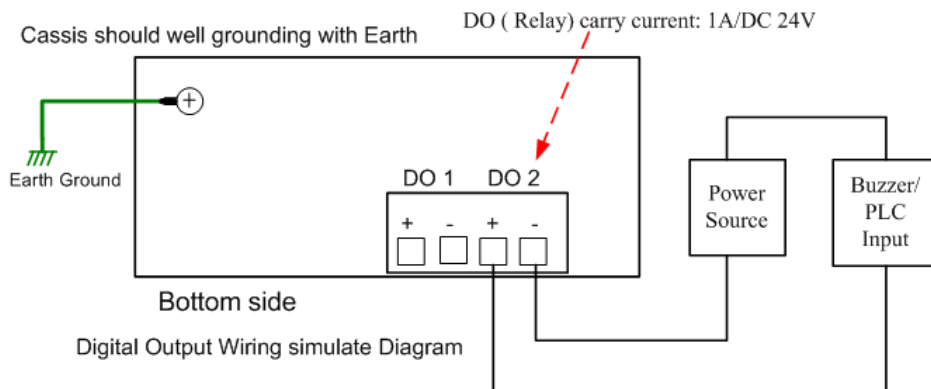
Wire the digital input just like wiring the power input introduced in chapter 2.2.



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.

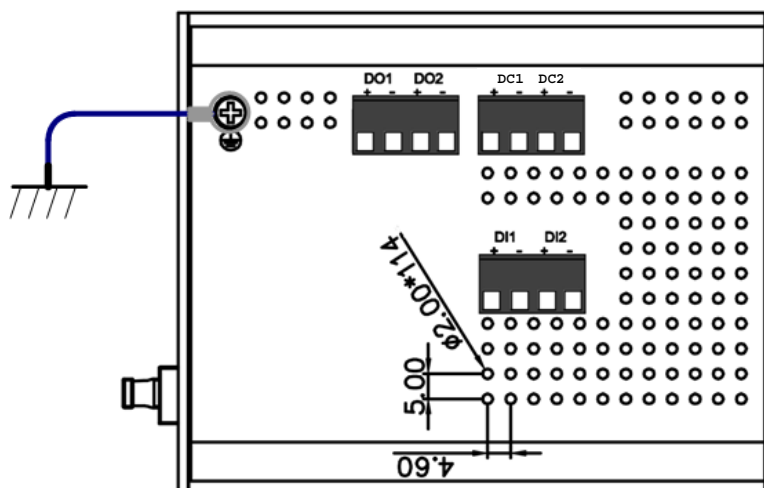
Wiring digital output is exactly the same as wiring power input introduced in chapter 2.2.



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.

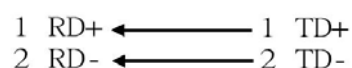
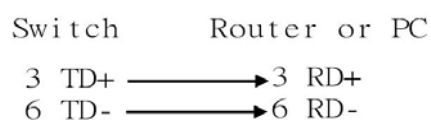
On the bottom side of the switch, there is one earth ground screw. Loosen the earth ground screw by screw driver; then tighten the screw after earth ground wire is connected.



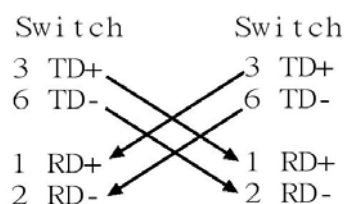
2.6 Wiring Fast Ethernet Ports

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 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 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 ranger from 550m to 80KM.

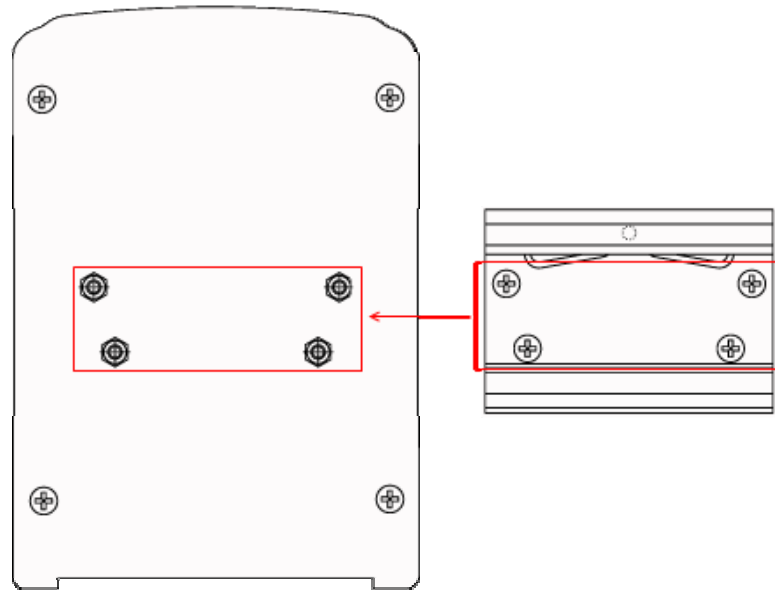
2.8 Wiring RS-232 Console Cable

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 CLI interface by console able.

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

2.9 DIN-Rail Mounting Installation

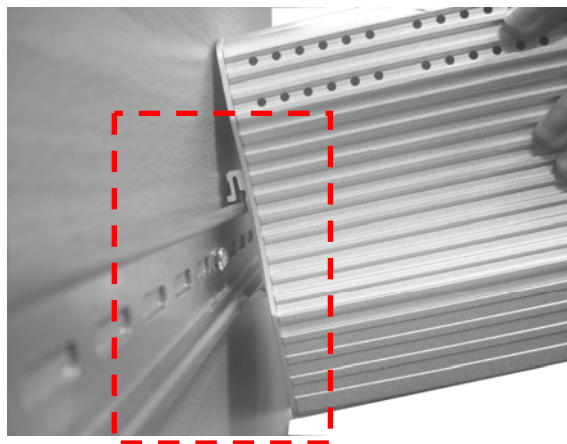
The DIN-Rail clip is already attached to the switch when packaged. If the DIN-Rail clip is not screwed on the switch, follow the instructions and the figure below to attach DIN-Rail clip to the switch.



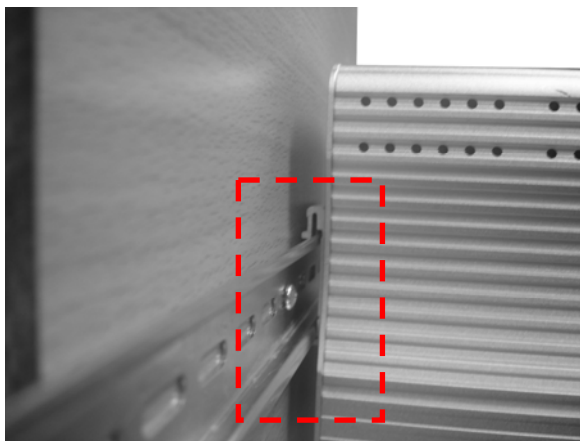
1. Use the screws to attach DIN-Rail clip to the rear panel.
2. To remove DIN-Rail clip, reverse step 1.

Follow the steps below to mount to the DIN-Rail track:

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



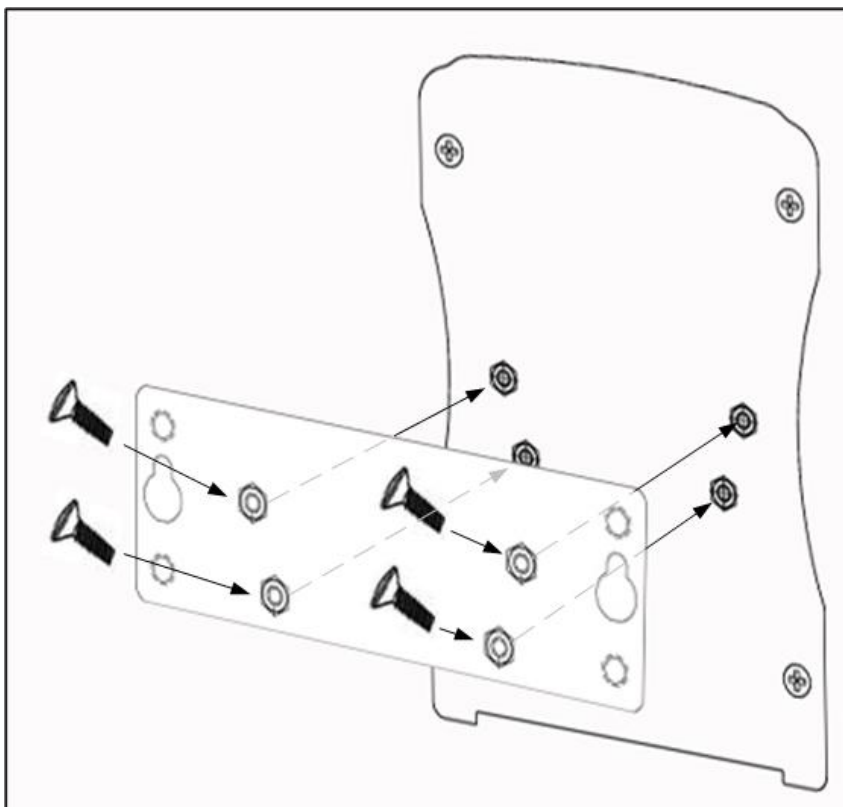
2. Lightly push the bottom of DIN-Rail clip into the track.



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

Notes: The DIN Rail should compliance with DIN EN50022 standard. Using wrong DIN rail may cause system install unsafe.

2.10 Wall-Mounting Installation



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

1. To remove DIN-Rail clip from the switch, loosen the screws from DIN-Rail clip.
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 and tight the wall-mount kit onto the rear side of the switch.
The specification of screw is M3 in 6 mm length.

2.11 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 øvrige ledere, se medfølgende installationsvejledning".

"Laite on liitettävä suojamaadoitus-koskettimilla varustettuun pistorasiaan"

„Apparatet må tilkoples jordet stikkontakt“

"Apparaten skall anslutas till jordat uttag"

3 Preparation for Management

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

Following topics are covered in this chapter:

3.1 Preparation for Serial Console

3.2 Preparation for Web Interface

3.3 Preparation for Telnet console

3.1 Preparation for Serial Console

In the package, 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 the cable, please follow the console cable PIN assignment to find one. (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. Login 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

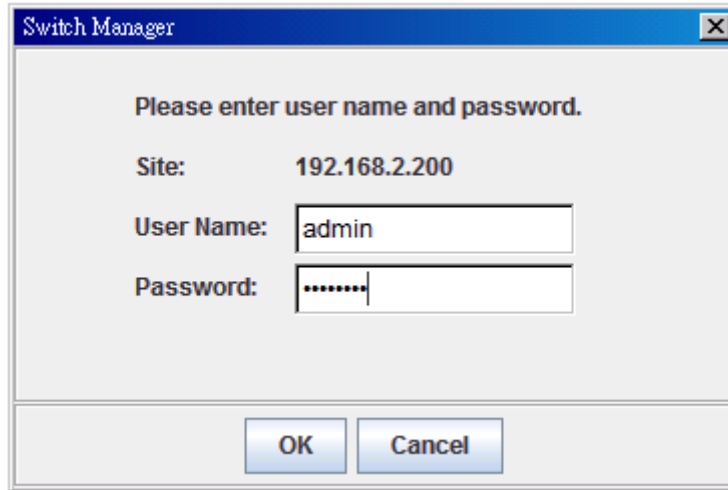
Westermo web management page is developed by JAVA. It allows you to use a standard web-browser such as Microsoft Internet Explorer, or Mozilla, to configure and interrogate the switch from anywhere on the network.

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 every 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. Key in user name and the password. Default user name is admin and password **westermo**.



Switch Manager

Please enter user name and password.

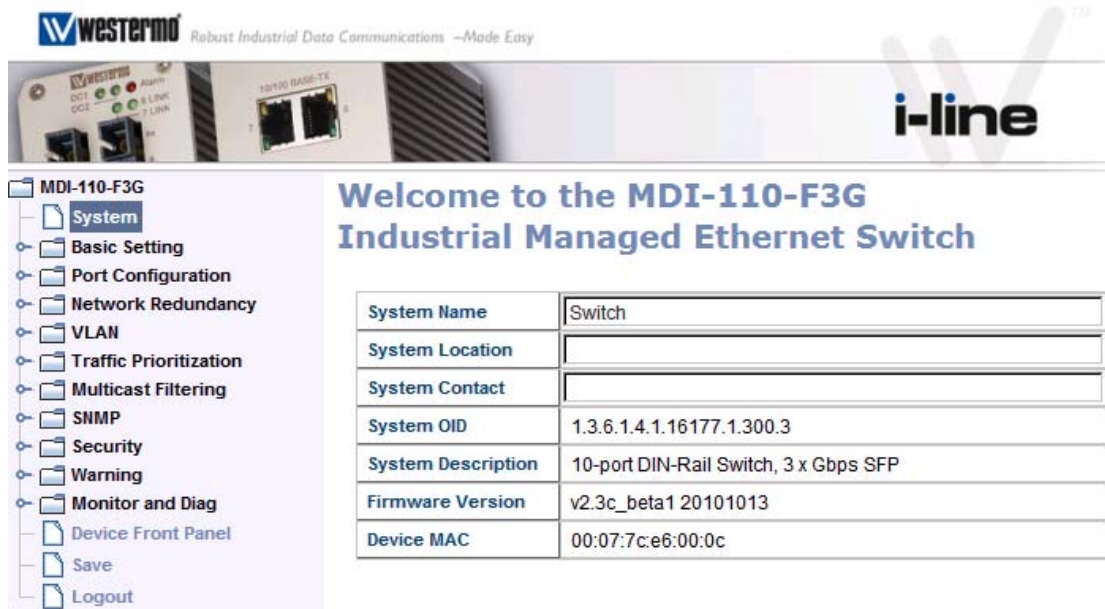
Site: 192.168.2.200

User Name:

Password:

OK Cancel

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



WESTERMO Robust Industrial Data Communications - Made Easy

i-line

Welcome to the MDI-110-F3G Industrial Managed Ethernet Switch

System Name	Switch
System Location	
System Contact	
System OID	1.3.6.1.4.1.16177.1.300.3
System Description	10-port DIN-Rail Switch, 3 x Gbps SFP
Firmware Version	v2.3c_beta1 20101013
Device MAC	00:07:7c:e6:00:0c

- MDI-110-F3G
 - System
 - Basic Setting
 - Port Configuration
 - Network Redundancy
 - VLAN
 - Traffic Prioritization
 - Multicast Filtering
 - SNMP
 - Security
 - Warning
 - Monitor and Diag
 - Device Front Panel
 - Save
 - Logout

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

Note 1: 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 key in correct user name and password again.

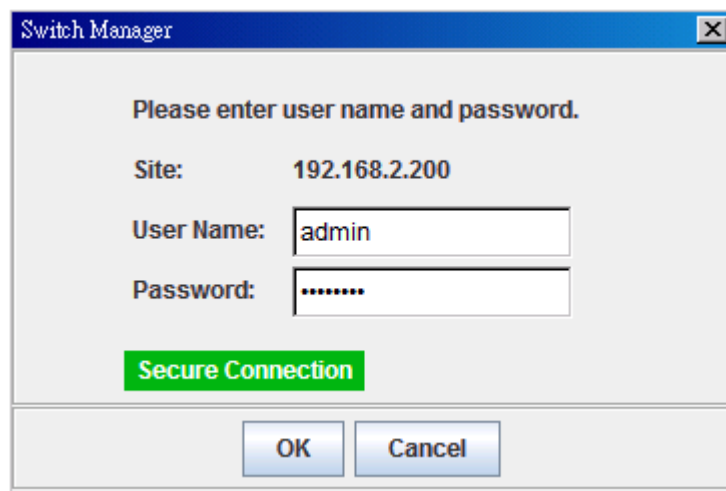
3.2.2 Secured Web Interface

Westermo web management page also provides secured management HTTPS

login. All the configuration commands will be secured and will be hard for the hackers to sniff the login password and configuration commands.

Launch the web browser and Login.

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

A screenshot of a Windows-style dialog box titled "Switch Manager". The dialog box has a blue title bar with a close button (X) in the top right corner. The main area is light gray and contains the text "Please enter user name and password." in bold. Below this text, there are three labels: "Site:", "User Name:", and "Password:". The "Site:" label is followed by the text "192.168.2.200". The "User Name:" label is followed by a text input field containing the text "admin". The "Password:" label is followed by a text input field containing seven dots. Below these input fields, there is a green button with the text "Secure Connection" in white. At the bottom of the dialog box, there are two buttons: "OK" and "Cancel".

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

3.3 Preparation for Telnet Console

3.3.1 Telnet

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

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

3.3.2 SSH (Secure Shell)

The switch also support SSH console. You can remotely connect to the switch

by command line interface. The SSH connection can secure all the configuration commands you sent to the switch.

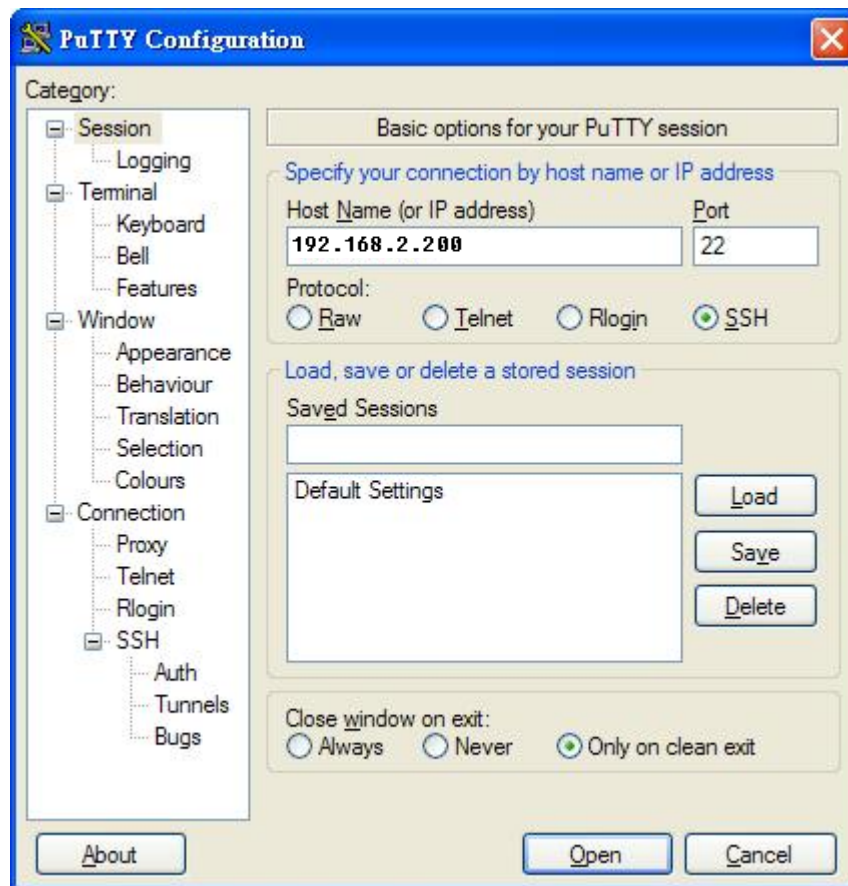
SSH is a client/server architecture while the switch is the SSH server. When you want to make SSH connection with the switch, you should download the SSH client tool first.

SSH Client

There are many free, sharewares, trials or charged SSH clients you can find on the internet. For 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.

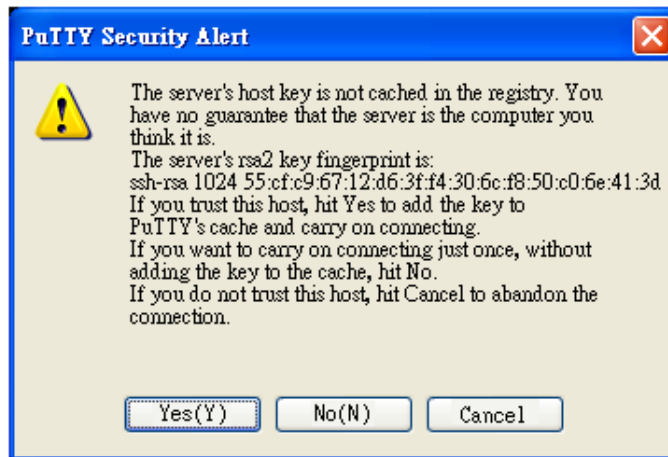
1. Open SSH Client/PuTTY

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, Web browser and SNMP.

Following topics are covered in this chapter:

- 4.1 Command Line Interface (CLI) Introduction
- 4.2 Basic Setting
- 4.3 Port Configuration
- 4.4 Network Redundancy
- 4.5 VLAN
- 4.6 Traffic Prioritization
- 4.7 Multicast Filtering
- 4.8 SNMP
- 4.9 Security
- 4.10 Warning
- 4.11 Monitor and Diag
- 4.12 Device Front Panel
- 4.13 Save
- 4.14 Logout

4.1 Command Line Interface Introduction

The Command Line Interface (CLI) is the user interface 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 keying in a command. There are some different command modes. Each command 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, (Port/VLAN) Interface Configuration modes.

User EXEC mode: As long as you login 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 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: Press 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: Press **configure terminal** in privileged EXEC mode. You can 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: Press **interface IFNAME** in global configuration mode. You can then enter interface configuration mode. In this mode, 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. You can then enter VLAN interface configuration mode. In this mode, 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
```

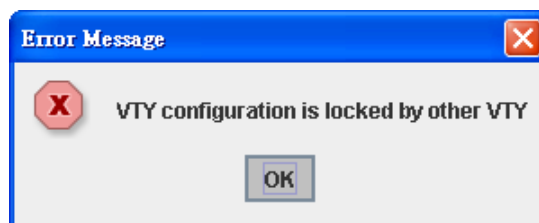
Ctrl+C To stop executing the unfinished command.

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 group:

- 4.2.1 Switch Setting
- 4.2.2 Admin Password
- 4.2.3 IP Configuration
- 4.2.4 Time Setting
- 4.2.5 DHCP Server
- 4.2.6 Backup and Restore
- 4.2.7 Firmware Upgrade
- 4.2.8 Factory Default
- 4.2.9 System Reboot
- 4.2.10 CLI Commands for Basic Setting

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 device. 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 Name	Switch
System Location	
System Contact	
System OID	1.3.6.1.4.1.16177.1.300.3
System Description	10-port DIN-Rail Switch, 3 x Gbps SFP
Firmware Version	v2.3c_beta1 20101013
Device MAC	00:07:7c:e6:00:0c

Apply

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.

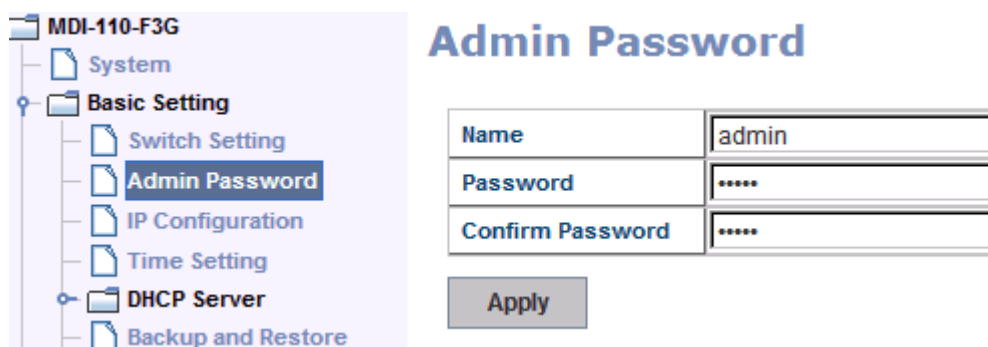
MAC Address: Display unique hardware address (MAC address) assigned by the manufacturer.

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



Admin Password	
Name	admin
Password
Confirm Password
<input type="button" value="Apply"/>	

Figure 4.2.2.1 Web UI of the Admin Password

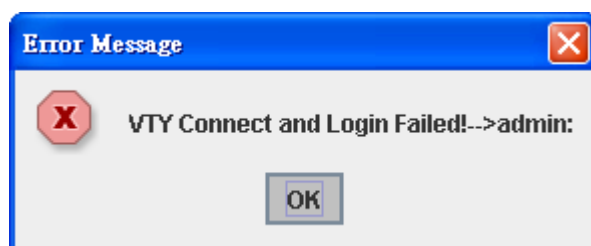
User name: You can key in new user name here. The default setting is **admin**.

Password: You can key in 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 Username.



4.2.3 IP Configuration

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

MDI-110-F3G

- System
- Basic Setting
 - Switch Setting
 - Admin Password
 - IP Configuration**
 - Time Setting
 - Jumbo Frame
- DHCP Server
- Backup and Restore

IP Configuration

DHCP Client Disable ▼

IP Address	192.168.0.119
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.254

Apply

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. The default gateway is 192.168.2.254. **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.

4.2.4 Time Setting

Time Setting source allow user to set the time manually or through NTP server. Network

Time Protocol (NTP) is used to synchronize computer clocks on the internet. You can configure NTP settings here to synchronize the clocks of several switches on the network.

It also provides Daylight Saving function.

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

NTP client: Select the Time Setting Source to NTP client can let device enable the NTP client service. NTP client will be automatically enabled if you change Time source to NTP Client. The system will send request packet to acquire current time from the NTP server you assigned.

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) Auckland, 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.

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.

DHCP Server configuration

DHCP Server Configuration

DHCP Server Enable ▼

DHCP Server Configuration

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

Apply

Excluded Address

IP Address	
------------	--

Add

Excluded Address List

Index	IP Address

Remove

Manual Binding

IP Address	
MAC Address	

Add

Manual Binding List

Index	IP Address	MAC Address

After

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

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

Excluded Address:

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

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

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

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

the **Reload** button to refresh the listing.

DHCP Leased Entries

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

Reload

DHCP Relay Agent

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

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 fill the field with preferred 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.

DHCP Relay Agent

Relay Agent ☒ Enable ☐ Disable

Relay Policy ☐ Relay policy drop
☐ Relay policy keep
☒ Relay policy replace

Helper Address 1	<input type="text"/>
Helper Address 2	<input type="text"/>
Helper Address 3	<input type="text"/>
Helper Address 4	<input type="text"/>

Apply

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

Backup and Restore

Backup Configuration		Local File ▼
Backup File Name	d:\backup.conf 	
<input type="button" value="Backup"/>		
Restore Configuration		TFTP Server ▼
TFTP Server IP	192.168.2.100	
Restore File Name	backup.conf	
<input type="button" value="Restore"/>		



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.


Firmware Upgrade

System Firmware Version: v1.1_beta2

System Firmware Date: 20101018-15:19:03

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

Firmware Upgrade Local File ▼

Firmware File Name 

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

Upgrade

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.

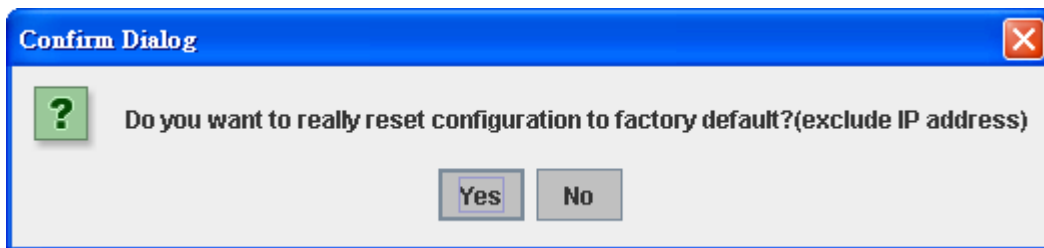
Click on **Upgrade** to start the process.

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.

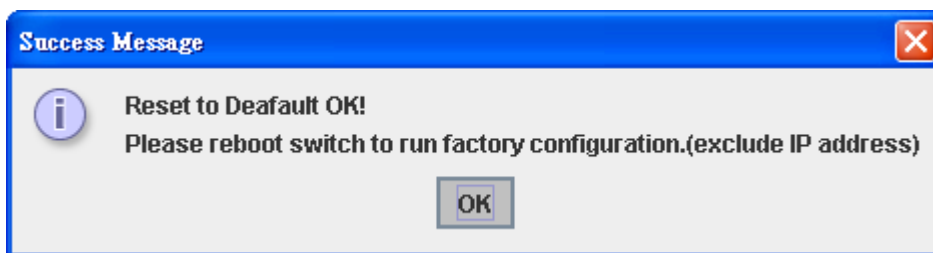
4.2.8 Factory Default

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.

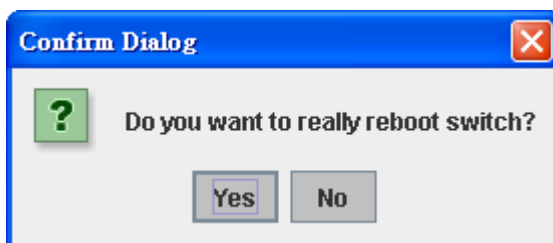
Note: If you already configured the IP of your device to other IP address, when you use this command by CLI and Web UI, our software will not reset the IP address to default IP. The system will remain the IP address so that you can still connect the switch via the network.

4.2.9 System Reboot

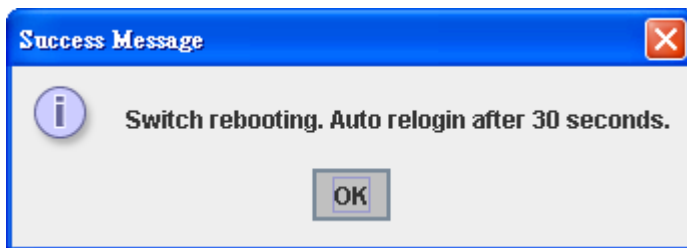
System Reboot allows you to reboot the device. Some of the feature changes require you to reboot the system. Click on **Reboot** to reboot your device.

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	<pre>Switch(config)# hostname WORD Network name of this system Switch(config)# hostname SWITCH SWITCH(config)#</pre>
System Location	<pre>SWITCH(config)# snmp-server location Sweden</pre>
System Contact	<pre>SWITCH(config)# snmp-server contact support@westermo.se</pre>
Display	<pre>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</pre>
Admin Password	
User Name and Password	<pre>SWITCH(config)# administrator NAME Administrator account name SWITCH(config)# administrator orwell PASSWORD Administrator account password SWITCH(config)# administrator orwell orwell Change administrator account orwell and password</pre>

	orwell success.
Display	<pre> SWITCH# show administrator Administrator account information name: orwell password: orwell </pre>
IP Configuration	
IP Address/Mask (192.168.2.8, 255.255.255.0	<pre> 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 </pre>
Gateway	<pre> SWITCH(config)# ip route 0.0.0.0/0 192.168.2.254/24 </pre>
Remove Gateway	<pre> SWITCH(config)# no ip route 0.0.0.0/0 192.168.2.254/24 </pre>
Display	<pre> 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 ! </pre>
Time Setting	
NTP Server	<pre> SWITCH(config)# ntp peer enable disable primary secondary SWITCH(config)# ntp peer primary IPADDR SWITCH(config)# ntp peer primary 192.168.2.200 </pre>
Time Zone	<pre> SWITCH(config)# clock timezone 26 Sun Jan 1 04:13:24 2006 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London </pre>

	Note: By typing clock timezone ?, you can see the timezone list. Then choose the number of the timezone you want to select.
Display	<pre> 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 </pre>
DHCP Server	
DHCP Server configuration	<pre> 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 </pre>
Lease time configure	<pre> Switch(config-dhcp)#lease 300 (300 sec) </pre>
DHCP Relay Agent	<pre> 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 </pre>

	<pre>Switch(config-dhcp)# ip dhcp relay information policy replace drop Relay Policy keep Drop/Keep/Replace option82 field replace</pre>
Show DHCP server information	<pre>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)</pre>
Backup and Restore	
Backup Startup Configuration file	<pre>Switch# copy startup-config tftp: 192.168.2.33/default.conf Writing Configuration [OK]</pre> <p>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.</p> <p>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</p>

	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 group:

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

4.3.1 Port Control

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

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

Apply

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-TX	Up	Enable	100 Full	Disable			--
2	100BASE-TX	Up	Enable	100 Full	Disable			--
3	100BASE-TX	Down	Enable	--	Disable			--
4	100BASE-TX	Down	Enable	--	Disable			--
5	100BASE-TX	Down	Enable	--	Disable			--
6	100BASE-TX	Down	Enable	--	Disable			--
7	100BASE-TX	Down	Enable	--	Disable			--
8	1000BASE	Down	Enable	--	Disable	--	--	--
9	1000BASE	Down	Enable	--	Disable	--	--	--
10	1000BASE	Down	Enable	--	Disable	--	--	--

SFP DDM

Port	Remove	Temperature (°C)		Tx Power (dBm)		Rx Power (dBm)	
		Current	Range	Current	Range	Current	Range
8	Eject	--	--	--	--	--	--
9	Eject	--	--	--	--	--	--
10	Eject	--	--	--	--	--	--

Reload

Eject All

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.

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

Temperature: The temperature specific 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 i-line 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 Control

Limit Packet Type and Rate

Port	Ingress Rule		Egress Rule	
	Packet Type	Rate(Mbps)	Packet Type	Rate(Mbps)
1	Broadcast Only ▼	8	All	0
2	Broadcast Only ▼	8	All	0
3	Broadcast Only ▼	8	All	0
4	Broadcast Only ▼	8	All	0
5	Broadcast Only ▼	8	All	0
6	Broadcast Only ▼	8	All	0
7	Broadcast Only ▼	8	All	0
8	Broadcast Only ▼	8	All	0
9	Broadcast Only ▼	8	All	0
10	Broadcast Only ▼	8	All	0

Apply

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. 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 in parallel 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 2 types of port trunking. One is Static Trunk, the other is 802.3ad. When the other end uses 802.3ad LACP, you **should** assign 802.3ad LACP to the trunk. When the other end uses non-802.3ad, you can then use Static Trunk.

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

Aggregation Setting

Port Trunk - Aggregation Setting

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

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

Apply

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.

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 LACP links well, 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	<p>Switch(config-if)# shutdown -> Disable port state</p> <p>Port1 Link Change to DOWN</p> <p>interface fastethernet1 is shutdown now.</p> <p>Switch(config-if)# no shutdown -> Enable port state</p> <p>Port1 Link Change to DOWN</p> <p>Port1 Link Change to UP</p> <p>interface fastethernet1 is up now.</p> <p>Switch(config-if)# Port1 Link Change to UP</p> <p>Switch(config)# sfp</p> <p>ddm Digital diagnostic and monitoring</p> <p>Switch(config)# sfp ddm</p> <p>Eject Reject DDM SFP</p>

	<p>Switch(config)# sfp ddm eject → eject SFP DDM transceiver all All DDM interface</p> <p>Example: Switch(config)# sfp ddm eject all</p> <p>DDM SFP on Port 9 normally ejected.</p> <p>DDM SFP on Port 9 normally ejected.</p> <p>All DDM SFP normally ejected.</p> <p>Switch(config)# interface gigabitethernet10 → eject port 10 SFP DDM transceiver.</p> <p>Switch(config-if)# sfp ddm eject</p> <p>DDM SFP on Port 10 normally ejected.</p>
Port Control - Auto Negotiation	<p>Switch(config)# interface fa1</p> <p>Switch(config-if)# auto-negotiation</p> <p>Auto-negotiation of port 1 is enabled!</p>
Port Control - Force Speed/Duplex	<p>Switch(config-if)# speed 100</p> <p>Port1 Link Change to DOWN</p> <p>set the speed mode ok!</p> <p>Switch(config-if)# Port1 Link Change to UP</p> <p>Switch(config-if)# duplex full</p> <p>Port1 Link Change to DOWN</p> <p>set the duplex mode ok!</p> <p>Switch(config-if)# Port1 Link Change to UP</p>
Port Control - Flow Control	<p>Switch(config-if)# flowcontrol on</p> <p>Flowcontrol on for port 1 set ok!</p> <p>Switch(config-if)# flowcontrol off</p> <p>Flow control off for port 1 set ok!</p>
Port Status	
Port Status	<p>Switch# show interface fa1</p> <p>Interface fastethernet1</p> <p>Administrative Status : Enable</p> <p>Operating Status : Connected</p> <p>Duplex : Full</p> <p>Speed : 100</p> <p>Flow Control :off</p> <p>Default Port VLAN ID: 1</p>

	<p>Ingress Filtering : Disabled</p> <p>Acceptable Frame Type : All</p> <p>Port Security : Disabled</p> <p>Auto Negotiation : Disable</p> <p>Loopback Mode : None</p> <p>STP Status: forwarding</p> <p>Default CoS Value for untagged packets is 0.</p> <p>Mdix mode is Disable.</p> <p>Medium mode is Copper.</p> <p>Switch# show sfp ddm →show SFP DDM information</p> <p>Port 8</p> <p>Temperature:N/A</p> <p>Tx power:N/A</p> <p>Rx power:N/A</p> <p>Port 9</p> <p>Temperature:64.00 C <range :0.0-80.00></p> <p>Tx power:-6.0 dBm <range : -9.0 - -4.0></p> <p>Rx power:-30.0 dBm <range: -30.0 - -4.0></p> <p>Port 10</p> <p>Temperature:67.00 C <range :0.0-80.00></p> <p>Tx power:-6.0 dBm <range : -9.0 - -4.0></p> <p>Rx power:-2.0 dBm <range: -30.0 - -4.0></p> <p>Note: Administrative Status -> Port state of the port.</p> <p>Operating status -> Current status of the port. Duplex -> Duplex mode of the port. Speed -> Speed mode of the port.</p> <p>Flow control -> Flow Control status of the port.</p>
Rate Control	
Rate Control - Ingress or Egress	<p>Switch(config-if)# rate-limit</p> <p>egress Outgoing packets</p> <p>ingress Incoming packets</p> <p>Note: To enable rate control, you should select the Ingress or Egress rule first; then assign the packet type and bandwidth.</p>
Rate Control - Filter Packet	<p>Switch(config-if)# rate-limit ingress mode</p> <p>all Limit all frames</p>

Type	<pre>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.</pre>
Rate Control - Bandwidth	<pre>Switch(config-if)# rate-limit ingress 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.</pre>
Port Trunking	
LACP	<pre>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.</pre>
Static Trunk	<pre>Switch(config)# trunk group 2 fa6-7 Trunk group 2 enable ok!</pre>
Display - LACP	<pre>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</pre>
Display - Trunk	<pre>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</pre>

	<p> FLAGS: I -> Individual P -> In channel D -> Port Down </p> <p>Trunk Group</p> <p>GroupID Protocol Ports</p> <p>-----+-----+-----</p> <p>2 Static 6(D) 7(P)</p> <p>Switch#</p>
--	--

4.4 Network Redundancy

It is critical for industrial applications that network remains non-stop. The switch firmware supports standard RSTP, Multiple Super Ring, Rapid Dual Homing.

Multiple Super Ring (MSR) technology ranks the fastest restore and failover time in the world, 0 ms for restore and about 5 milliseconds for failover for copper.

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 couple 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 group:

- 4.4.1 RSTP
- 4.4.2 RSTP Info
- 4.4.3 Multiple Super Ring
- 4.4.4 Ring Info
- 4.4.5 Command Lines for Network Redundancy

4.4.1 RSTP

RSTP is the abbreviation of Rapid Spanning Tree Protocol. If a switch has more than one path to a destination, it will lead to message loops that can generate broadcast storms and quickly bog down a network. The spanning tree was created to combat the negative effects of message loops in switched networks. A spanning tree uses a spanning tree algorithm (STA) to automatically sense whether a switch has more than one way to communicate with a node. It will then select the best path (primary), and block the other path(s). It will also keep track of the blocked path(s) in case the primary path fails. Spanning Tree Protocol (STP) introduced a standard method to accomplish this. It is specified in IEEE 802.1D-1998. Later, Rapid Spanning Tree Protocol (RSTP) was adopted and represents the evolution of STP, providing much faster spanning tree convergence after a topology change. This is specified in IEEE 802.1w. In 2004, 802.1w is included into 802.1D-2004 version. This switch supports both RSTP and STP (all switches that support RSTP are also backward compatible with switches that support only STP).

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

MDI-110-F3G

- System
- Basic Setting
- Port Configuration
- Network Redundancy
 - RSTP**
 - RSTP Information
 - Multiple Super Ring
 - Multiple Super Ring Infor
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
- Warning
- Monitor and Diag
 - Device Front Panel
 - Save
 - Logout

Rapid Spanning Tree Protocol

RSTP Enable ▼

Bridge Configuration

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

Port Configuration

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

Apply

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

Bridge Configuration

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

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

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

If the switch is not the root bridge, and if it has not received a hello message from the root bridge in an amount of time equal to Max Age, then 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.

$2 \times (\text{Forward Delay Time} - 1 \text{ sec}) \geq \text{Max Age Time} \geq 2 \times (\text{Hello Time value} + 1 \text{ sec})$

Port Configuration

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

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

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

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

means to auto select P2P or Share mode. “**P2P**” means P2P is enabled, while “**Share**” means P2P is disabled.

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

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

4.4.2 RSTP Info

RSTP Information

Root Information

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

Port Information

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

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

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

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

4.4.3 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.

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

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 automatically naming with Ring ID.

Multiple Super Ring

New Ring

Ring ID	Name
<input type="text"/>	<input type="text"/>

Add

Ring Configuration

ID	Name	Version	Device Priority	Ring Port1	Path Cost	Ring Port2	Path Cost	Rapid Dual Homing	Ring Status
1	Ring1	Rapid Super Ring	128	Port 9	128	Port 10	128	Disable	Enable

Apply Remove Reload

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

Ring Port1: In Rapid Super Ring environment, you should have 2 Ring Ports. No matter this switch is Ring Master or not, when configuring RSR, 2 ports should be selected to be Ring Ports. For Ring Master, one of the ring ports will become the forwarding port and the other one will become the blocking port.

Path Cost: Change the Path Cost of Ring Port1. If this switch is the Ring Master of

a Ring, then it determines the blocking port. The Port with higher Path Cost in the two 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 an important 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 7 multiple links for redundancy without any problem.

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

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

4.4.4 Ring Info

This page shows the RSR information.

Multiple Super Ring Information

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

[Reload](#)

ID: Ring ID.

Version: which version of this ring, this field could be Rapid Super Ring, Super Ring.

Role: This Switch is RM or nonRM

Status: If this field is Normal which means the redundancy is approved. If any one of the link in this Ring is broken, 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 means how many times the Ring status has been transformed between Normal and Abnormal state.

4.4.5 Command Lines:

Feature	Command Line
RSTP	
Enable	Switch(config)# spanning-tree enable
Disable	Switch (config)# spanning-tree disable
RSTP mode	Switch(config)# spanning-tree mode rapid-stp SpanningTree Mode change to be RSTP(802.1w) .
STP mode	Switch(config)# spanning-tree mode stp SpanningTree Mode change to be STP(802.1d) .
Priority	Switch(config)# spanning-tree priority <0-61440> valid range is 0 to 61440 in multiple of 4096 Switch(config)# spanning-tree priority 4096
Max Age	Switch(config)# spanning-tree max-age <6-40> Valid range is 6~40 seconds Switch(config)# spanning-tree max-age 10
Hello Time	Switch(config)# spanning-tree hello-time <1-10> Valid range is 1~10 seconds Switch(config)# spanning-tree hello-time 2
Forward Delay	Switch(config)# spanning-tree forward-time <4-30> Valid range is 4~30 seconds Switch(config)# spanning-tree forward-time 15
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																														
RSTP Info																															
Active status	Switch# show spanning-tree active Rapid Spanning-Tree feature Enabled Spanning-Tree BPDU transmission-limit 3 Root Address 0007.7c01.0386 Priority 4096 Root Path Cost : 200000 Root Port : 7 Root Times : max-age 20 sec, hello-time 2 sec, forward-delay 15 sec Bridge Address 0007.7cff.0102 Priority 4096 Bridge Times : max-age 10 sec, hello-time 2 sec, forward-delay 15 sec Aging time : 300 <table><tr><td>Port</td><td>Role</td><td>Port-State</td><td>Cost</td><td>Prio.Nbr</td></tr><tr><td>Type</td><td></td><td></td><td></td><td></td></tr><tr><td colspan="5">-----</td></tr><tr><td colspan="5">-----</td></tr><tr><td>fa6</td><td>Designated</td><td>Forwarding</td><td>200000</td><td>128.6</td></tr></table> Auto(RST) <table><tr><td>fa7</td><td>Root</td><td>Forwarding</td><td>200000</td><td>128.7</td></tr></table> Shared(STP)	Port	Role	Port-State	Cost	Prio.Nbr	Type					-----					-----					fa6	Designated	Forwarding	200000	128.6	fa7	Root	Forwarding	200000	128.7
Port	Role	Port-State	Cost	Prio.Nbr																											
Type																															

fa6	Designated	Forwarding	200000	128.6																											
fa7	Root	Forwarding	200000	128.7																											
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 <table><tr><td>Blocking</td><td>Listening</td><td>Learning</td><td>Forwarding</td><td>Disabled</td></tr><tr><td colspan="5">-----</td></tr><tr><td>0</td><td>0</td><td>0</td><td>2</td><td>8</td></tr></table> #Port Link-Type Summary <table><tr><td>AutoDetected</td><td>PointToPoint</td><td>SharedLink</td><td>EdgePort</td></tr><tr><td colspan="4">-----</td></tr></table>	Blocking	Listening	Learning	Forwarding	Disabled	-----					0	0	0	2	8	AutoDetected	PointToPoint	SharedLink	EdgePort	-----										
Blocking	Listening	Learning	Forwarding	Disabled																											

0	0	0	2	8																											
AutoDetected	PointToPoint	SharedLink	EdgePort																												

	9 0 1 9
Port Info	Switch# show spanning-tree port detail fa7 (Interface_ID) Rapid Spanning-Tree feature Enabled Port 128.6 as Disabled Role is in Disabled State Port Path Cost 200000, Port Identifier 128.6 RSTP Port Admin Link-Type is Auto, Oper Link-Type is Point-to-Point RSTP Port Admin Edge-Port is Enabled, Oper Edge-Port is Edge Designated root has priority 32768, address 0007.7c00.0112 Designated bridge has priority 32768, address 0007.7c60.1aec Designated Port ID is 128.6, Root Path Cost is 600000 Timers : message-age 0 sec, forward-delay 0 sec Link Aggregation Group: N/A, Type: N/A, Aggregated with: N/A BPDU: sent 43759 , received 4854 TCN : sent 0 , received 0 Forwarding-State Transmit count 12 Message-Age Expired count
Multiple Super Ring	
Create or configure a Ring	Switch(config)# multiple-super-ring 1 Ring 1 created Switch(config-multiple-super-ring)# Note: 1 is the target Ring ID which is going to be created or configured.
Super Ring Version	Switch(config-multiple-super-ring)# version default set default to rapid super ring rapid-super-ring rapid super ring super-ring super ring Switch(config-multiple-super-ring)# version rapid-super-ring
Priority	Switch(config-multiple-super-ring)# priority

	<p><0-255> valid range is 0 to 255</p> <p>default set default</p> <p>Switch(config)# super-ring priority 100</p>
Ring Port	<p>Switch(config-multiple-super-ring)# port</p> <p>IFLIST Interface list, ex: fa1,fa3-5,gi8-10</p> <p>cost path cost</p> <p>Switch(config-multiple-super-ring)# port fa1,fa2</p>
Ring Port Cost	<p>Switch(config-multiple-super-ring)# port cost</p> <p><0-255> valid range is 0 or 255</p> <p>default set default (128)valid range is 0 or 255</p> <p>Switch(config-multiple-super-ring)# port cost 100</p> <p><0-255> valid range is 0 or 255</p> <p>default set default (128)valid range is 0 or 255</p> <p>Switch(config-super-ring-plus)# port cost 100 200</p> <p>Set path cost success.</p>
Rapid Dual Homing	<p>Switch(config-multiple-super-ring)#</p> <p>rapid-dual-homing enable</p> <p>Switch(config-multiple-super-ring)#</p> <p>rapid-dual-homing disable</p> <p>Switch(config-multiple-super-ring)#</p> <p>rapid-dual-homing port</p> <p>IFLIST Interface name, ex: fastethernet1 or gi8</p> <p>auto-detect up link auto detection</p> <p>IFNAME Interface name, ex: fastethernet1 or gi8</p> <p>Switch(config-multiple-super-ring)#</p> <p>rapid-dual-homing port fa3,fa5-6</p> <p>set Rapid Dual Homing port success.</p> <p>Note: auto-detect is recommended for dual Homing..</p>
Ring Info	
Ring Info	<p>Switch# show multiple-super-ring [Ring ID]</p> <p>[Ring1] Ring1</p> <p>Current Status : Disabled</p> <p>Role : Disabled</p> <p>Ring Status : Abnormal</p> <p>Ring Manager : 0000.0000.0000</p> <p>Blocking Port : N/A</p>

	<p>Giga Copper : N/A</p> <p>Configuration :</p> <p>Version : Rapid Super Ring</p> <p>Priority : 128</p> <p>Ring Port : fa1, fa2</p> <p>Path Cost : 100, 200</p> <p>Dual-Homing II : Disabled</p> <p>Statistics :</p> <table><tr><td>Watchdog sent</td><td>0, received</td><td>0, missed</td><td>0</td></tr><tr><td>Link Up sent</td><td>0, received</td><td>0</td><td></td></tr><tr><td>Link Down sent</td><td>0, received</td><td>0</td><td></td></tr></table> <p>Role Transition count 0</p> <p>Ring State Transition count 1</p> <p>Ring ID is optional. If the ring ID is typed, this command will only display the information of the target Ring.</p>	Watchdog sent	0, received	0, missed	0	Link Up sent	0, received	0		Link Down sent	0, received	0	
Watchdog sent	0, received	0, missed	0										
Link Up sent	0, received	0											
Link Down sent	0, received	0											

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, this also saves a lot of computing resources within the switch.

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

Following commands are included in this group:

- 4.5.1 VLAN Port Configuration
- 4.5.2 VLAN Configuration
- 4.5.3 GVRP Configuration
- 4.5.4 VLAN Table
- 4.5.5 CLI Commands of the VLAN

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.

MDI-110-F3G

- System
- Basic Setting
- Port Configuration
- Network Redundancy
 - RSTP
 - RSTP Information
 - Multiple Super Ring
 - Multiple Super Ring Inforr
- VLAN**
 - VLAN Port Configuration**
 - VLAN Configuration
 - GVRP Configuration
 - VLAN Table
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
- Warning
- Monitor and Diag

VLAN Port Configuration

VLAN Port Configuration

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

PVID: The abbreviation of the **Port VLAN ID**. Enter port VLAN ID here. 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 2 PVIDs. 1 is the default value. 2 to 4094 are valid and available in this column. Type the PVID you'd like to configure here.

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

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

4.5.2 VLAN Configuration

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

Figure 4.5.2.1 Web UI of the VLAN Configuration.

VLAN Configuration

Management VLAN ID

Static VLAN

VLAN ID	Name
<input type="text"/>	<input type="text"/>

Static VLAN Configuration

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

Management VLAN ID: The switch supports management VLAN. The management VLAN ID is the VLAN ID of the CPU interface so that only member ports of the management VLAN can ping and 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. 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.

Static VLAN Configuration

VLAN ID	Name	1	2	3	4	5	6	7	8	9	10
1	VLAN1	U	U	U	U	U	U	U	U	U	U
2	VLAN2	-	-	-	-	T	T	T	T	-	-
3	test	U	U	U	U	-	-	-	-	-	-

Figure 4.5.2.4 Configure Egress rule of the ports.

-- : Not available

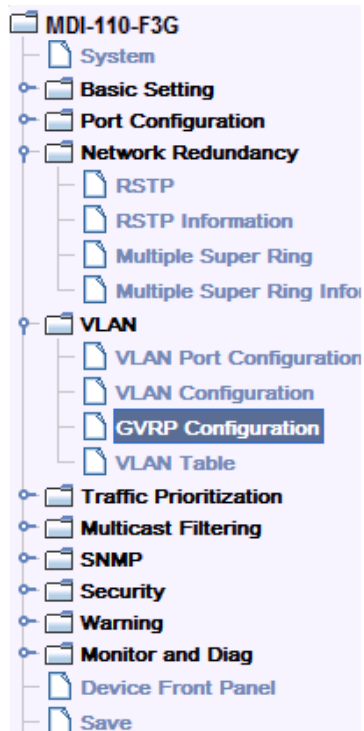
U : Untag: Indicates that egress/outgoing frames are not VLAN tagged.

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 Configuration

GVRP Protocol ▼

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

Note: Timer unit is centiseconds.

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

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

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

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

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

4.5.4 VLAN Table

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

VLAN Table

VLAN Table

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

Reload

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	
VLAN Port PVID	Switch(config-if)# switchport trunk native vlan 2 Set port default vlan id to 2 success
Port Accept Frame Type	Switch(config)# inter fa1 Switch(config-if)# acceptable frame type all any kind of frame type is accepted! Switch(config-if)# acceptable frame type vlantaggedonly only vlan-tag frame is accepted!
Ingress Filtering	Switch(config)# interface fa1

(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 Type)	Switch# show interface fa1 Interface fastethernet1 Administrative Status : Enable Operating Status : Not Connected Duplex : Auto Speed : Auto Flow Control :off Default Port VLAN ID: 2 Ingress Filtering : Disabled Acceptable Frame Type : All Port Security : Disabled Auto Negotiation : Enable Loopback Mode : None STP Status: disabled Default CoS Value for untagged packets is 0. Mdix mode is Auto. Medium mode is Copper.
Display - Port Egress Rule (Egress rule, IP address, status)	Switch# show running-config ! interface fastethernet1 switchport access vlan 1 switchport access vlan 3 switchport trunk native vlan 2 interface vlan1 ip address 192.168.2.8/24 no shutdown
VLAN Configuration	
Create VLAN (2)	Switch(config)# vlan 2

	<p>vlan 2 success</p> <p>Switch(config)# interface vlan 2 Switch(config-if)#</p> <p>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.</p>
Remove VLAN	<p>Switch(config)# no vlan 2 no vlan success</p> <p>Note: You can only remove the VLAN when the VLAN is in unused mode.</p>
VLAN Name	<p>Switch(config)# vlan 2 vlan 2 has exists Switch(config-vlan)# name v2</p> <p>Switch(config-vlan)# no name</p> <p>Note: Use no name to change the name to default name, VLAN VID.</p>
VLAN description	<p>Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# description this is the VLAN 2</p> <p>Switch(config-if)# no description ->Delete the description.</p>
IP address of the VLAN	<p>Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# ip address 192.168.2.200/24</p> <p>Switch(config-if)# no ip address 192.168.2.200/24 ->Delete the IP address</p>
Create multiple VLANs (VLAN 5-10)	Switch(config)# interface vlan 5-10
Shut down VLAN	<p>Switch(config)# interface vlan 2 Switch(config-if)# shutdown</p>

	Switch(config-if)# no shutdown ->Turn on the VLAN
Display - VLAN table	Switch# sh vlan VLAN Name Status Trunk Ports Access Ports ----- ----- 1 VLAN1 Static - fa1-7,gi8-10 2 VLAN2 Unused - - 3 test Static fa4-7,gi8-10 fa1-3,fa7,gi8-10
Display - VLAN interface information	Switch# show interface vlan1 interface vlan1 is up, line protocol detection is disabled index 14 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST> HWaddr: 00:07:7c:ff:01:b0 inet 192.168.2.200/24 broadcast 192.168.2.255 input packets 639, bytes 38248, dropped 0, multicast packets 0 input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0 output packets 959, bytes 829280, dropped 0 output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0 collisions 0
GVRP configuration	
GVRP enable/disable	Switch(config)# gvrp mode disable Disable GVRP feature globally on the switch enable Enable GVRP feature globally on the switch Switch(config)# gvrp mode enable Gvrp is enabled on the switch!
Configure GVRP timer	Switch(config)# inter fa1 Switch(config-if)# garp timer <10-10000>
Join timer /Leave timer/ LeaveAll	Switch(config-if)# garp timer 20 60 1000 Note: The unit of these timer is centisecond

timer	
Management VLAN	
Management VLAN	Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# no shutdown
Display	Switch# show running-config ! interface vlan1 ip address 192.168.2.200/24 ip igmp no shutdown !

4.6 Traffic Prioritization

Quality of Service (QoS) provides traffic prioritization mechanism which allows users to deliver better service to certain flows. QoS 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 4 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 group:

- 4.6.1 QoS Setting
- 4.6.2 CoS-Queue Mapping
- 4.6.3 DSCP-Queue Mapping
- 4.6.4 CLI Commands of the Traffic Prioritization

4.6.1 QoS Setting

QoS Setting

Queue Scheduling

☒ Use an 8,4,2,1 weighted fair queuing scheme

☐ Use a strict priority scheme

Port Setting

Port	CoS	Trust Mode
1	0	COS Only
2	0	COS Only
3	0	COS Only
4	0	COS Only
5	0	COS Only
6	0	COS Only
7	0	COS Only
8	0	COS Only
9	0	COS Only
10	0	COS Only

Apply

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.

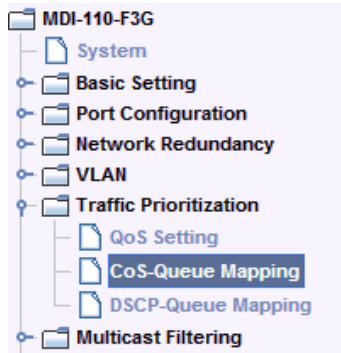
Default priority type is **COS Only**. The system will provide default COS-Queue table to which you can refer for the next command.

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

4.6.2 CoS-Queue Mapping

This page is to change CoS values to Physical Queue mapping table. Since the switch fabric only supports 4 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. 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.



CoS-Queue Mapping

CoS-Queue Mapping

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

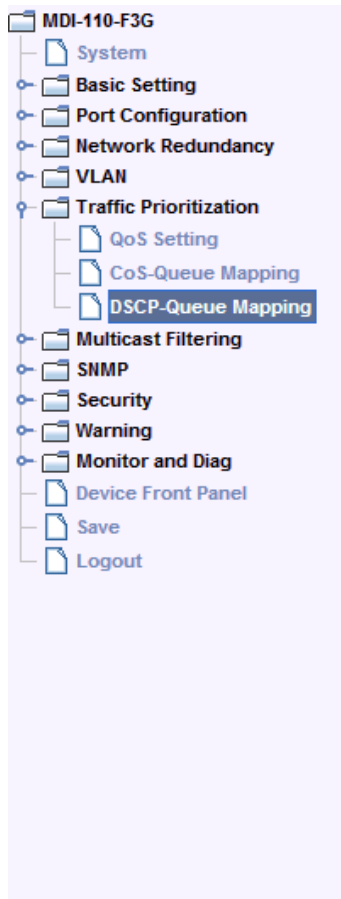
Note: Queue 3 is the highest priority queue.

Apply

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

4.6.3 DSCP-Queue Mapping

This page is to change DSCP values to Physical Queue mapping table. Since the switch fabric supports 4 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.



Traffic Prioritization

DSCP-Queue Mapping

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

Note: Queue 3 is the highest priority queue.

Apply

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

4.6.4 CLI Commands of the Traffic Prioritization

Command Lines of the Traffic Prioritization configuration

Feature	Command Line
QoS Setting	
Queue Scheduling - Strict Priority	<pre>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></pre>
Queue Scheduling - WRR	<pre>Switch(config)# qos queue-sched wrr</pre>
Port Setting - CoS (Default Port Priority)	<pre>Switch(config)# interface fal 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: fal means fast Ethernet port 1.</pre>
Port Setting - Trust Mode- CoS Only	<pre>Switch(config)# interface fal Switch(config-if)# qos trust cos The port trust is set CoS only ok.</pre>
Port Setting - Trust Mode- CoS First	<pre>Switch(config)# interface fal Switch(config-if)# qos trust cos-first The port trust is set CoS first ok.</pre>
Port Setting - Trust Mode- DSCP Only	<pre>Switch(config)# interface fal Switch(config-if)# qos trust dscp The port trust is set DSCP only ok.</pre>
Port Setting - Trust Mode- DSCP First	<pre>Switch(config)# interface fal Switch(config-if)# qos trust dscp-first The port trust is set DSCP first ok.</pre>
Display - Queue Scheduling	<pre>Switch# show qos queue-sched QoS queue scheduling scheme : Weighted Round Robin (Use an 8,4,2,1 weight)</pre>
Display - Port Setting - Trust Mode	<pre>Switch# show qos trust QoS Port Trust Mode : Port Trust Mode -----+-----</pre>

	<pre> 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 </pre>
Display - Port Setting - CoS (Port Default Priority)	<pre> 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 </pre>
CoS-Queue Mapping	
Format	<pre> 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 </pre>
Map CoS 0 to Queue 1	<pre> Switch(config)# qos cos-map 0 1 The CoS to queue mapping is set ok. </pre>
Map CoS 1 to Queue 0	<pre> Switch(config)# qos cos-map 1 0 The CoS to queue mapping is set ok. </pre>
Map CoS 2 to Queue 0	<pre> Switch(config)# qos cos-map 2 0 The CoS to queue mapping is set ok. </pre>

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 1 0 0

	1 0 0 0 0 0 0 0 0 0 0 0 0
	2 0 0 0 0 1 1 1 1 1 1 1 1
	3 1 1 2 2 2 2 2 2 2 2 2 2
	4 2 2 2 2 2 2 2 2 2 2 3 3
	5 3 3 3 3 3 3 3 3 3 3 3 3
	6 3 3 3 3

4.7 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 or not.

Following commands are included in this group:

- 4.7.1 IGMP Snooping
- 4.7.2 IGMP Query
- 4.7.3 Force Filtering
- 4.7.4 CLI Commands of the Multicast Filtering

4.7.1 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.

MDI-110-F3G

- System
- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
 - QoS Setting
 - CoS-Queue Mapping
 - DSCP-Queue Mapping
- Multicast Filtering**
 - IGMP Snooping**
 - IGMP Query
 - Unknown Multicast
- SNMP
- Security
- Warning
- Monitor and Diag
- Device Front Panel

IGMP Snooping

IGMP Snooping Disable ▼

Apply

	VID	IGMP Snooping
<input type="checkbox"/>	1	Disabled

☐ Select All

Enable Disable

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.

IGMP Snooping Table

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

Reload

4.7.2 IGMP Query

MDI-110-F3G

System

Basic Setting

Port Configuration

Network Redundancy

VLAN

Traffic Prioritization

Multicast Filtering

IGMP Snooping

IGMP Query

Unknown Multicast

IGMP Query

IGMP Query on the Management VLAN

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

Apply

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 becomes 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.

4.7.3 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 learnt is so-called unknown multicast, the switch decide how to forward them based on the setting of this page.

Unknown Multicast

Unknown Multicast

- ☒ Send to Query Ports
- ☐ Send to All Ports
- ☐ Discard

Apply

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. It is usually the uplink port of the switch.

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

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

4.7.4 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 snooping IGMP snooping is disabled globally ok.
Disable IGMP Snooping -	Switch(config)# no ip igmp snooping vlan 3

VLAN	IGMP snooping is disabled on VLAN 3.
Display - IGMP Snooping Setting	<pre>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</pre>
Display - IGMP Table	<pre>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,</pre>
IGMP Query	
IGMP Query V1	<pre>Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# ip igmp v1</pre>
IGMP Query V2	<pre>Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# ip igmp</pre>
IGMP Query version	<pre>Switch(config-if)# ip igmp version 1 Switch(config-if)# ip igmp version 2</pre>
Disable	<pre>Switch(config)# int vlan 1 Switch(config-if)# no ip igmp</pre>
Display	<pre>Switch# sh ip igmp interface vlan1 enabled: Yes version: IGMPv2 query-interval: 125s query-max-response-time: 10s Switch# show running-config</pre>

	<pre> ... ! interface vlan1 ip address 192.168.2.200/24 ip igmp no shutdown ! </pre>
Unknown Multicast	
<pre> Unknown Multicast - Enable Force filtering (Send to All Ports) Disable Force filtering (Discard) </pre>	<pre> 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! </pre>
<pre> Unknown Multicast - Send to All Ports </pre>	<pre> Switch(config)# ip igmp snooping source-only-learning </pre>

4.8 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP 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 group:

- 4.8.1 SNMP Configuration
- 4.8.2 SNMPv3 Profile
- 4.8.3 SNMP Traps
- 4.8.4 SNMP CLI Commands for SNMP

4.8.1 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 2 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 4 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.

MDI-110-F3G

- System
- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
 - SNMP Configuration
 - SNMP V3 Profile
 - SNMP Traps
- Security

SNMP

SNMP V1/V2c Community

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

Apply

4.8.2 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.

MDI-110-F3G

- System
- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
 - SNMP Configuration
 - SNMP V3 Profile
 - SNMP Traps
- Security
 - Warning
 - Monitor and Diag
 - Device Front Panel
 - Save
 - Logout

SNMP V3 Profile

SNMP V3

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

Add

SNMP V3 Users

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

Remove Reload

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 2 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.

4.8.3 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.

MDI-110-F3G

- System
- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
 - SNMP Configuration
 - SNMP V3 Profile
 - SNMP Traps**
- Security
- Warning
- Monitor and Diag
 - MAC Address Table
 - Port Statistics
 - Port Mirroring
 - Event Log
 - Topology Discovery
 - Ping
- Device Front Panel
- Save
- Logout

SNMP Trap

SNMP Trap Enable ▼

Apply

SNMP Trap Server

Server IP	192.168.2.111
Community	public
Version	<input checked="" type="radio"/> V1 <input type="radio"/> V2c

Add

Trap Server Profile

Server IP	Community	Version
192.168.2.100	private	V2c

Remove Reload

4.8.4 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

4.9 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 group:

- 4.9.1 Port Security
- 4.9.2 IP Security
- 4.9.3 IEEE 802.1x
- 4.9.4 CLI Commands of the Security

4.9.1 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 environment and not 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. So the system can accept 100 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.

MDI-110-F3G

- System
- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
 - Port Security**
 - IP Security
 - 802.1x
- Warning
- Monitor and Diag
- Device Front Panel
- Save
- Logout

Port Security

Port Security State

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

Apply

Add Port Security Entry

Port	VID	MAC Address
Port 1		

Add

Port Security List

All

Port	VID	MAC Address
------	-----	-------------

Remove

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

4.9.2 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. Max security IP is 10.

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

MDI-110-F3G

- System
- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security**
 - Port Security
 - IP Security**
 - 802.1x
- Warning
- Monitor and Diag
- Device Front Panel
- Save
- Logout

IP Security

IP Security Enable ▼

Apply

Add Security IP

Security IP

Add

Security IP List

Index	Security IP
1	192.168.2.222

Remove Reload

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

4.9.3 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. With the function, the switch could control which connection is available or not.

802.1x Port-Based Network Access Control Configuration

System Auth Control

Authentication Method

Radius Server

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

Secondary Radius Server

RADIUS Server IP	
Shared Key	
Server Port	
Accounting Port	

Local Radius User

Username	Password	VID

Local Radius User List

Username	Password	VID

System AuthControl: To enable or disable the 802.1x authentication.

Authentication Method: Radius is a authentication server that provide key for authentication, with this method, user must connect switch to server. If user select Local for the authentication method, switch use the local user data base which can be 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 Radius server.

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

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

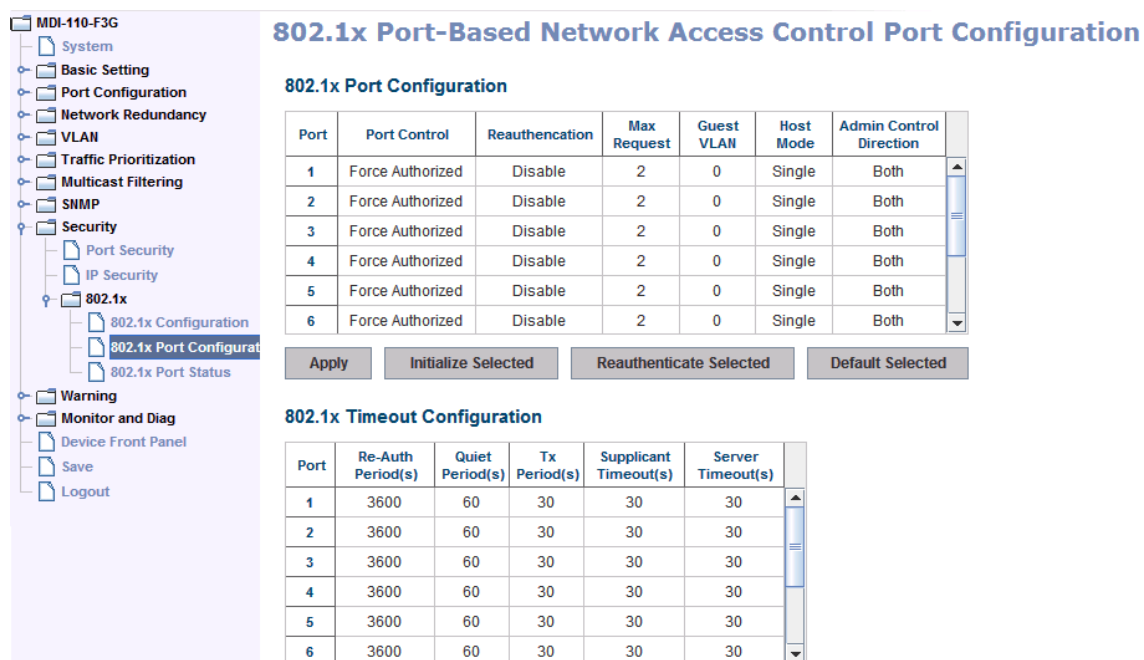
802.1X Local User: Here User can add Account/Password for local authentication.

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.



802.1x Port-Based Network Access Control Port Configuration

802.1x Port Configuration

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

Buttons: Apply, Initialize Selected, Reauthenticate Selected, Default Selected

802.1x Timeout Configuration

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

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: 0 to 4094 is available for this field. If this field is set to 0, that means the port is blocked after authentication fail. Otherwise, the port will be set to 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

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

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

Reload

4.9.4 CLI Commands of the Security

Command Lines of the Security configuration

Feature	Command Line
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 192.168.2.33 Add ip security host 192.168.2.33 ok.
Display	Switch# show ip security ip security is enabled ip security host: 192.168.2.33
802.1x	
enable diable	Switch(config)# dot1x system-auth-control Switch(config)# Switch(config)# no dot1x system-auth-control Switch(config)#
authentic-method	Switch(config)# dot1x authentic-method local Use the local username database for authentication radius Use the Remote Authentication Dial-In User Service (RADIUS) servers for authentication Switch(config)# dot1x authentic-method radius Switch(config)#
radius server-ip	Switch(config)# dot1x radius Switch(config)# dot1x radius server-ip 192.168.2.200 key 1234

	RADIUS Server Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) RADIUS Server IP : 192.168.2.200 RADIUS Server Key : 1234 RADIUS Server Port : 1812 RADIUS Accounting Port : 1813 Switch(config)#
radius server-ip	Switch(config)# dot1x radius Switch(config)# dot1x radius server-ip 192.168.2.200 key 1234 RADIUS Server Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) RADIUS Server IP : 192.168.2.200 RADIUS Server Key : 1234 RADIUS Server Port : 1812 RADIUS Accounting Port : 1813 Switch(config)#
radius secondary-server-ip	Switch(config)# dot1x radius secondary-server-ip 192.168.2.250 key 5678 Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) Secondary RADIUS Server IP : 192.168.2.250 Secondary RADIUS Server Key : 5678 Secondary RADIUS Server Port : 1812 Secondary RADIUS Accounting Port : 1813
User name/password for authentication	Switch(config)# dot1x username Westermo passwd Westermo vlan 1

4.10 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 group:

- 4.10.1 Fault Relay
- 4.10.2 Event Selection
- 4.10.3 Syslog Configuration
- 4.10.4 SMTP Configuration
- 4.10.5 CLI Commands

4.10.1 Fault Relay

The switch provides 2 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. 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. You should also configure them. Currently, each Relay can have one event type.

MDI-110-F3G

- System
- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
- Warning
 - Fault Relay**
 - Event & Email Warning
- Monitor and Diag
- Device Front Panel
- Save
- Logout

Fault Relay Setting

☒ **Relay 1**

Event Type	DI state
DI Number	DI 1
DI State	High

☒ **Relay 2**

Event Type	DI state
DI Number	DI state Dry Output Power Failure Link Failure Ping Failure Super Ring Failure
DI State	

Apply

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 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 a open circuit.

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

<input checked="" type="checkbox"/> Relay 1	
Event Type	Dry Output ▼
On Period(Sec)	1
Off Period(Sec)	0

Turn on the relay output

<input checked="" type="checkbox"/> Relay 2	
Event Type	Dry Output ▼
On Period(Sec)	0
Off Period(Sec)	1

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.

<input checked="" type="checkbox"/> Relay 1	
Event Type	Power Failure ▼
Power ID	Power DC1 ▼
	Power DC1
	Power DC2
	Any

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 linked down or broken, the system will short Relay Output and light the DO LED.

<input checked="" type="checkbox"/> Relay 1										
Event Type	Link Failure ▼									
Link	1	2	3	4	5	6	7	8	9	10
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	11	12	13	14	15	16	17	18		
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

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.

<input checked="" type="checkbox"/> Relay 1	
Event Type	Ping Failure ▼
IP Address	192.168.2.100
Reset Time(Sec)	5
Hold Time(Sec)	50

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.

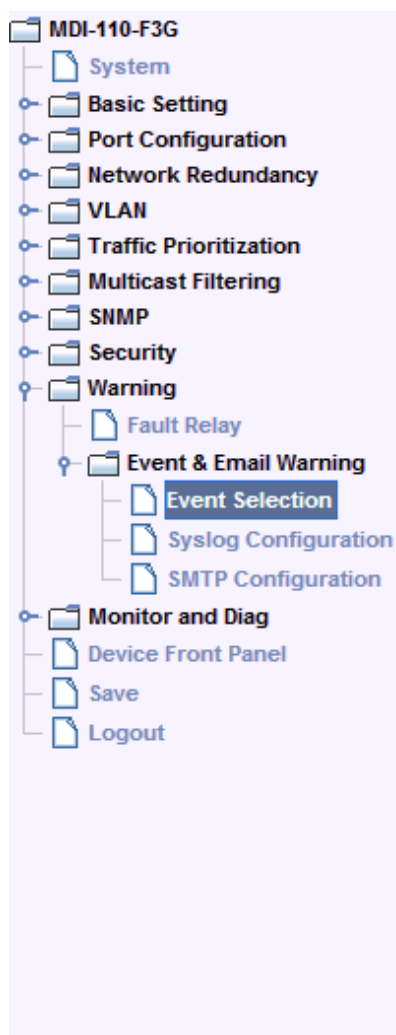
<input checked="" type="checkbox"/> Relay 1	
Event Type	Super Ring Failure ▼

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

4.10.2 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.
Super Ring Topology Changes	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.
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.



Warning - Event Selection

System Event Selection

- | | |
|---|---|
| <input type="checkbox"/> Device Cold Start | <input type="checkbox"/> Device Warm Start |
| <input type="checkbox"/> Power 1 Failure | <input type="checkbox"/> Power 2 Failure |
| <input type="checkbox"/> Authentication Failure | <input type="checkbox"/> Time Synchronize Failure |
| <input type="checkbox"/> Fault Relay | <input type="checkbox"/> Super Ring Topology Change |
| <input type="checkbox"/> SFP DDM Failure | <input type="checkbox"/> DI1 Change <input type="checkbox"/> DI2 Change |

Port Event Selection

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

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

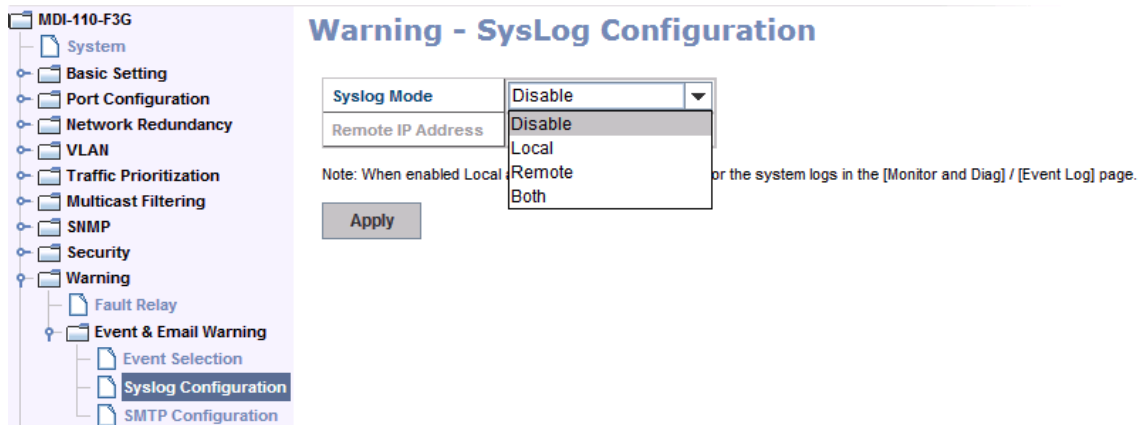
4.10.3 SysLog Configuration

System Log is useful to provide system administrator locally or remotely monitor switch events history. There are 2 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: Above 2 modes can be enabled at the same time.



Warning - SysLog Configuration

Syslog Mode:

Remote IP Address:

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

Apply

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.

4.10.4 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.



Warning - SMTP Configuration

E-mail Alert:

SMTP Configuration

SMTP Server IP	192.168.0.1
Mail Account	user@192.168.0.1
<input type="checkbox"/> Authentication	
User Name	
Password	
Confirm Password	
Rcpt E-mail Address 1	
Rcpt E-mail Address 2	
Rcpt E-mail Address 3	
Rcpt E-mail Address 4	

Apply

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.

4.10.5 CLI Commands

Command Lines of the Warning configuration

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

	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 192.168.2.33 <cr> reset reset a device Switch(config)# relay 1 ping 192.168.2.33 reset <1-65535> reset time Switch(config)# relay 1 ping 192.168.2.33 reset 60 <0-65535> hold time to retry Switch(config)# relay 1 ping 192.168.2.33 reset 60 60
Port Link Failure	Switch(config)# relay 1 port PORTLIST port list Switch(config)# relay 1 port fal-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 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 192.168.2.33
Both	Switch(config)# log syslog local Switch(config)# log syslog remote 192.168.2.33

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.
Dispaly	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:

4.11 Monitor and Diag

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

Following commands are included in this group:

4.11.1 MAC Address Table

4.11.2 Port Statistics

4.11.3 Port Mirror

4.11.4 Event Log

4.11.5 Topology Discovery

4.11.5 Ping

4.11.6 CLI Commands of the Monitor and Diag

4.11.1 MAC Address Table

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

Aging Time (Sec)

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

Static Unicast MAC Address

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

MAC Address Table

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

Packet Types: Management Unicast means MAC address of the switch. It belongs to CPU port only. **Static Unicast** MAC address can be added and deleted.

Dynamic Unicast MAC is MAC address learnt by the switch Fabric. **Static**

Multicast can be added by CLI and can be deleted by Web and CLI. **Dynamic Multicast** will appear after you enabled IGMP and the switch learnt IGMP report. Click on **Remove** to remove the static Unicast/Multicast MAC address. Click on **Reload** to refresh the table. New learnt Unicast/Multicast MAC address will be updated to MAC address table.

MAC Address Table

Aging Time (Sec)

Static Unicast MAC Address

MAC Address	VID	Port
<input type="text"/>	<input type="text"/>	<input type="text" value="Port 1"/>

MAC Address Table

MAC Address	Address Type	VID	1	2	3	4	5	6	7	8	9	10
0007.7ce6.0001	Dynamic Unicast	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
001d.725a.df26	Dynamic Unicast	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4.11.2 Port Statistics

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

Note: If you see many Bad, Abort or Collision counts increased, that may mean your network cable is not connected well, the network performance of the port is poor...etc. Please check your network cable, Network Interface Card of the connected device, the network application, or reallocate the network traffic...etc. Click on **Clear Selected** to reinitialize the counts of the selected ports, and **Clear All** to reinitialize the counts of all ports. Click on **Reload** to refresh the counts.

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

Clear Selected Clear All Reload

4.11.3 Port Mirroring

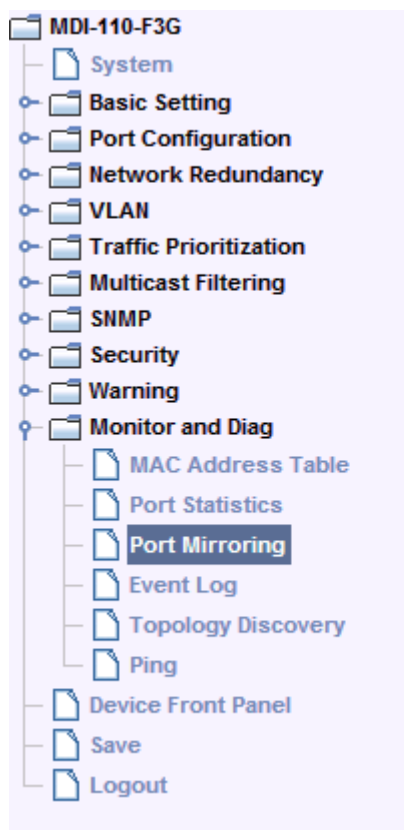
Port mirroring (also called port spanning) is a tool that allows you to mirror the traffic from one or more ports onto another port, without disrupting the flow of traffic on the original port. Any traffic that goes into or out of the Source Port(s) will be duplicated at the Destination Port. This traffic can then be analyzed at 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. 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 or Netxray device to this port.

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



Port Mirroring

Port Mirror Mode

Enable ▼

Port Selection

Port	Source Port		Destination Port	
	Rx	Tx	Rx	Tx
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>

Apply

4.11.4 Event Log

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

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

System Event Logs

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

Clear Reload

4.11.5 Topology Discovery

MDI-110-F3G

- System
- Basic Setting
- Port Configuration
- Network Redundancy
- VLAN
- Traffic Prioritization
- Multicast Filtering
- SNMP
- Security
- Warning
- Monitor and Diag
 - MAC Address Table
 - Port Statistics
 - Port Mirroring
 - Event Log
 - Topology Discovery**
 - Ping
- Device Front Panel
- Save
- Logout

LLDP Enable ▼

LLDP Configuration

LLDP timer	30
LLDP hold time	120

LLDP Port State

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

Apply

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 learnt 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.

4.11.6 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.

Ping Utility

Ping

Target IP	192.168.2.100
<input type="button" value="Start"/>	

Result

```
64 bytes from 192.168.2.100: icmp_seq=0 ttl=64 time=10.0 ms
64 bytes from 192.168.2.100: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 192.168.2.100: icmp_seq=2 ttl=64 time=0.0 ms
64 bytes from 192.168.2.100: icmp_seq=3 ttl=64 time=0.0 ms
64 bytes from 192.168.2.100: icmp_seq=4 ttl=64 time=0.0 ms

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

4.11.7 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.ffffa 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 ---- - -----

	<pre> 1 0100.5e40.0800 0 fa6-7 1 0100.5e7f.ffff 0 fa4,fa6-7 </pre>
Show MAC Address Table - Static MAC addresses	<pre> 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 </pre>
Show Aging timeout time	<pre> Switch# show mac-address-table aging-time the mac-address-table aging-time is 300 sec. </pre>
Port Statistics	
Port Statistics	<pre> 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, Disacrd: 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 </pre>
Port Mirroring	
Enable Port Mirror	<pre> Switch(config)# mirror en Mirror set enable ok. </pre>
Disable Port	<pre> Switch(config)# mirror disable </pre>

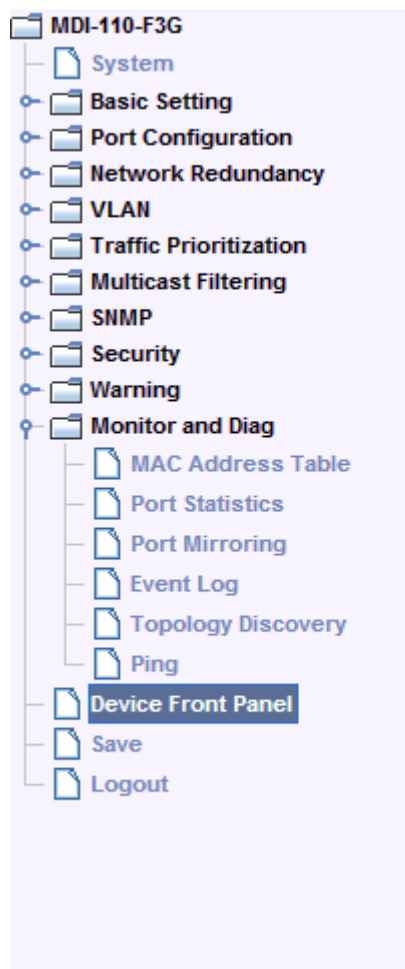
Mirror	Mirror set disable ok.
Select Source Port	Switch(config)# mirror source fa1-2 both Received and transmitted traffic rx Received traffic tx Transmitted traffic Switch(config)# mirror source fa1-2 both Mirror source fa1-2 both set ok. Note: Select source port list and TX/RX/Both mode.
Select Destination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

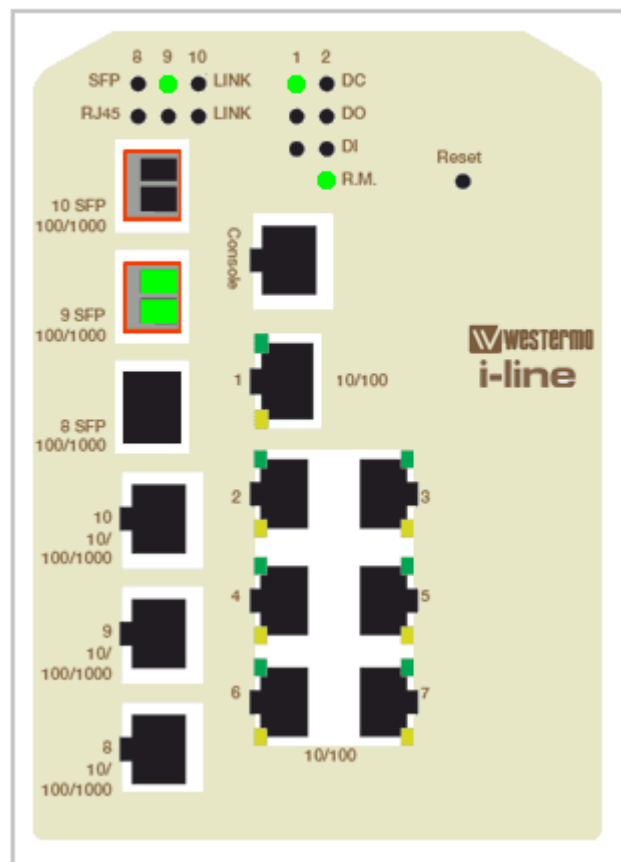
4.12 Device Front Panel

Device Front Panel command allows you to see LED status of 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.



Device Front Panel



Note: No CLI command for this feature.

4.13 Save to Flash

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

Command Lines:

Feature	Command Line
Save	<pre>SWITCH# write Building Configuration... [OK] Switch# copy running-config startup-config Building Configuration... [OK]</pre>

4.14 Logout

The switch provides 2 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:

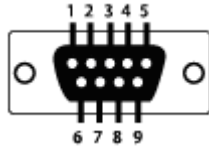
Feature	Command Line
Logout	SWITCH> exit
	SWITCH# exit

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

5.2 Private MIB

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

5.3 Revision History

Edition	Date	Modifications
V0.1	2010/10/11	The first version



Westermo Teleindustri AB • SE-640 40 Stora Sundby, Sweden

Phone +46 16 42 80 00 Fax +46 16 42 80 01

E-mail: info@westermo.se

Westermo Web site: www.westermo.com

Subsidiaries

Westermo Data Communications AB

Svalgängen 1

SE-724 81 Västerås

Phone: +46 (0)21 548 08 00 • Fax: +46 (0)21 35 18 50

E-mail: info.sverige@westermo.se

Westermo Data Communications Ltd

Talisman Business Centre • Duncan Road

Park Gate, Southampton • SO31 7GA

Phone: +44(0)1489 580-585 • Fax: +44(0)1489 580586

E-Mail: sales@westermo.co.uk

Westermo Data Communications GmbH

Goethestraße 67, 68753 Waghäusel

Tel.: +49(0)7254-95400-0 • Fax: +49(0)7254-95400-9

E-Mail: info@westermo.de

Westermo Data Communications S.A.R.L.

9 Chemin de Chilly 91160 CHAMPLAN

Tél : +33 1 69 10 21 00 • Fax : +33 1 69 10 21 01

E-mail: infos@westermo.fr

Westermo Data Communications Pte Ltd

2 Soon Wing Road #08-05

Soon Wing Industrial Building

Singapore 347893

Phone +65 6743 9801 • Fax +65 6745 0670

E-Mail: sales@westermo.com.sg

Westermo Teleindustri AB have distributors in several countries, contact us for further information.