Cisco ME 1200 Series Carrier Ethernet Access Device Web Interface User Guide, Cisco IOS 15.6(1)SN and Later Releases

First Published: 2016-02-05

Last Modified: 2018-02-07

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 3

CHAPTER 4

CHAPTER 5

CHAPTER 6

CHAPTER 7

Preface

This preface contains information about the Cisco ME 1200 Series Carrier Ethernet Access Device.

Audience

This guide is for the person configuring the Cisco ME 1200 Series Carrier Ethernet Access Devices, hereafter known as Cisco ME 1200 NID.

Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands and keywords and user-entered text appear in **bold** font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`Courier font`	Terminal sessions and information the system displays appear in `courier` font.
`Bold Courier font`	Bold Courier font indicates text that the user must enter.
[x]	Elements in square brackets are optional.

Convention	Description
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
{x | y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document uses the following conventions for reader alerts:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means *the following information will help you solve a problem.*

Warning **Means *reader be warned.* In this situation, you might perform an action that could result in bodily injury.**

Related Documentation

These documents provide information about the switches and are available from this Cisco.com site:

http://www.cisco.com/c/en/us/support/switches/me-1200-series-carrier-ethernet-access-devices/tsd-products-support-general-information.html

- *Release Notes for the Cisco ME 1200 Series Carrier Ethernet Access Devices*

  Note Before installing, configuring, or upgrading the switch, see the release notes on Cisco.com for the latest information.

- *Cisco ME 3800x and ME 3600x Switches Software Configuration Guide*
- *Cisco Regulatory Compliance and Safety Information for Cisco ME 1200 Series Carrier Ethernet Access Devices*

For information on supported MIBs, see ftp://ftp.cisco.com/pub/mibs/ME1200-MIBS/.

CHAPTER 1

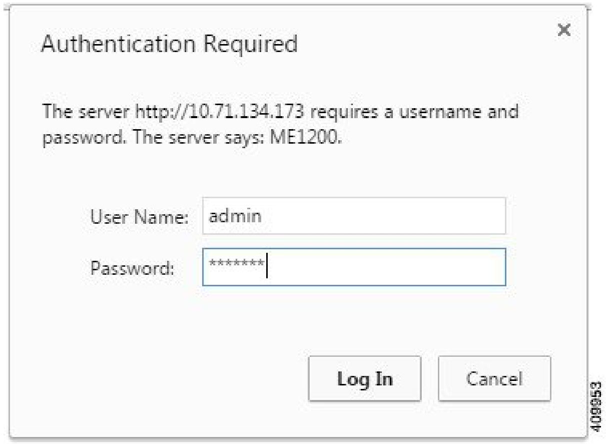
Basic Functionality

This section describes the basic functionality of the ME 1200 Web GUI interface.

Logging in to the Web GUI

The following assumes the Cisco ME 1200 device is powered on and has a functional connection to a computer using the serial console port on the device (115200 baud, No parity, 8 data bits, 1 stop bit, no flow control), as well as a connection from the computer's LAN port to a copper port on the device. The computer must be running a terminal emulator such as TeraTerm or PuTTY on Windows or Minicom on Linux.

Configure your computer's LAN port to an address in the same subnet as the ME 1200 device. Open your browser and enter the IP address of the device (**You may have to turn off your wireless receiver or adjust your firewall settings.)



Authentication Required

The server http://10.71.134.173 requires a username and password. The server says: ME1200.

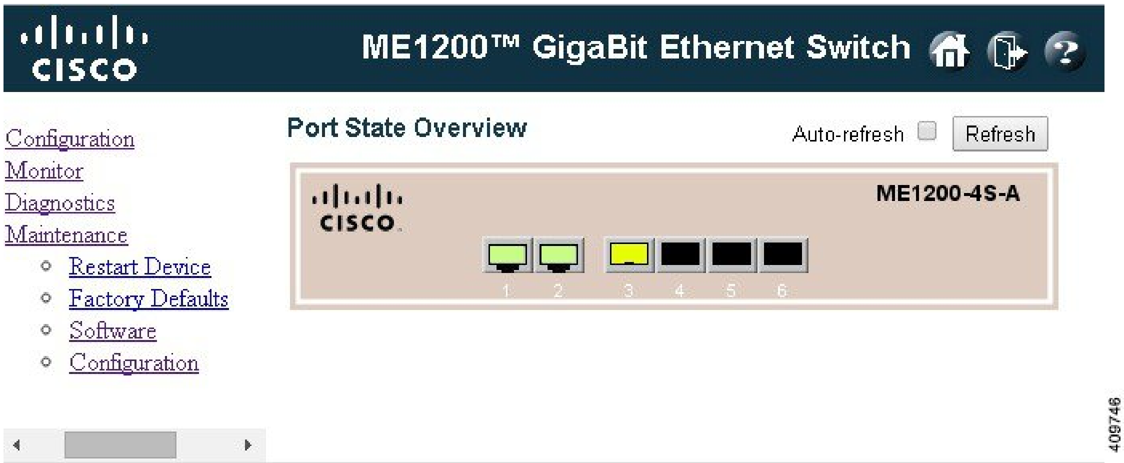
User Name: admin

Password: *******

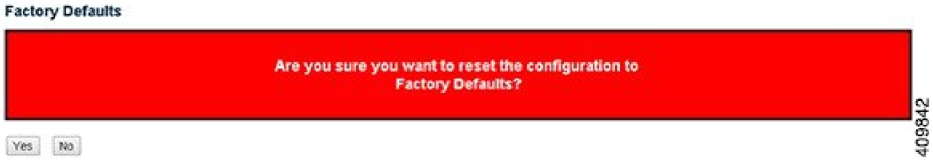
Enter the same default username and password into the popup box.

Reset Configuration to Factory Defaults

Once you have access to the online GUI, you will see a list of links on the left side of the page. Click on **Maintenance** > **Factory Defaults**.



Confirm that you want to reset the configuration to factory defaults.



Are you sure you want to reset the configuration to Factory Defaults?

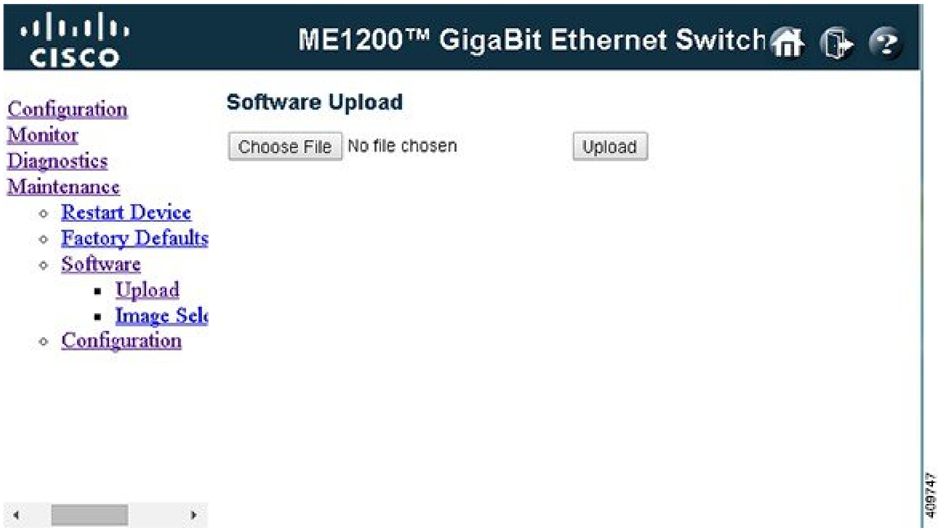
You will then see a confirmation message the reset has been completed.

Related Topics

Factory Defaults, on page 251

Software Upgrade

To perform a software upgrade, save the new image on your computer. In the left panel of the GUI, click **Maintenance** > **Software** > **Upload**.

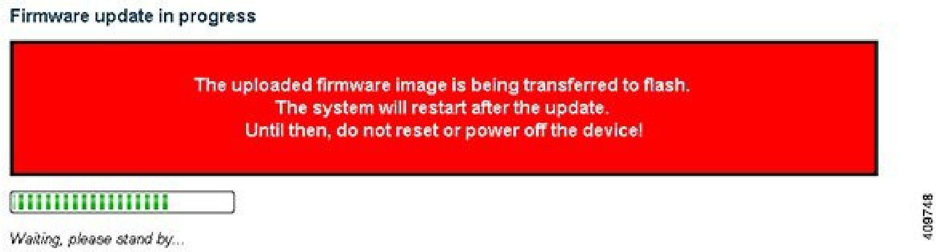


Software Upload

Choose File No file chosen

Upload

Click **Choose File** and select the new image. Then click **Upload**. You will see a confirmation message and a status bar showing the progress of the firmware upgrade.



Firmware update in progress

The uploaded firmware image is being transferred to flash.
The system will restart after the update.
Until then, do not reset or power off the device!

Waiting, please stand by...

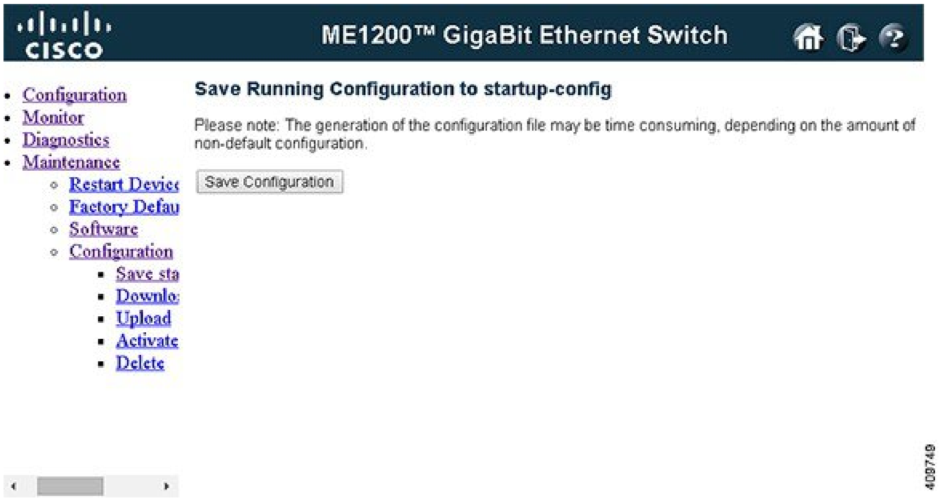
The box will automatically reboot when finished. You may also switch to an alternate image already loaded onto the box by clicking **Image Select** under **Software**.

Related Topics

Software Upload, on page 252

Display and Save Configuration to FLASH

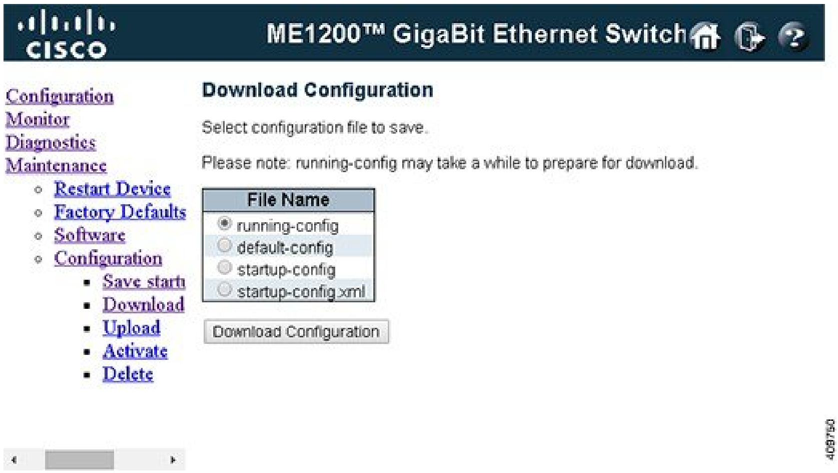
To save the configuration to flash, click **Maintenance** > **Configuration** > **Save startup-config**.



Save Running Configuration to startup-config

Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

To display the configuration, click **Maintenance** > **Configuration** > **Download**. Choose the configuration you want to download, and click **Download Configuration**.



Download Configuration

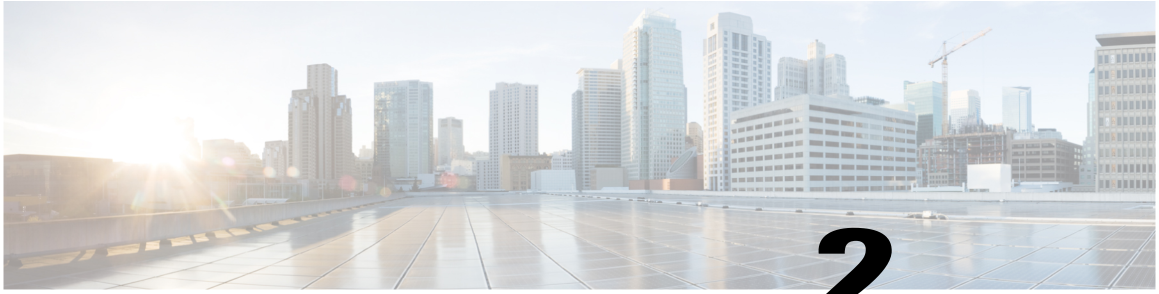
Select configuration file to save.

Please note: running-config may take a while to prepare for download.

File Name
● running-config
○ default-config
○ startup-config
○ startup-config.xml

Related Topics

Maintaining Configuration Files, on page 254



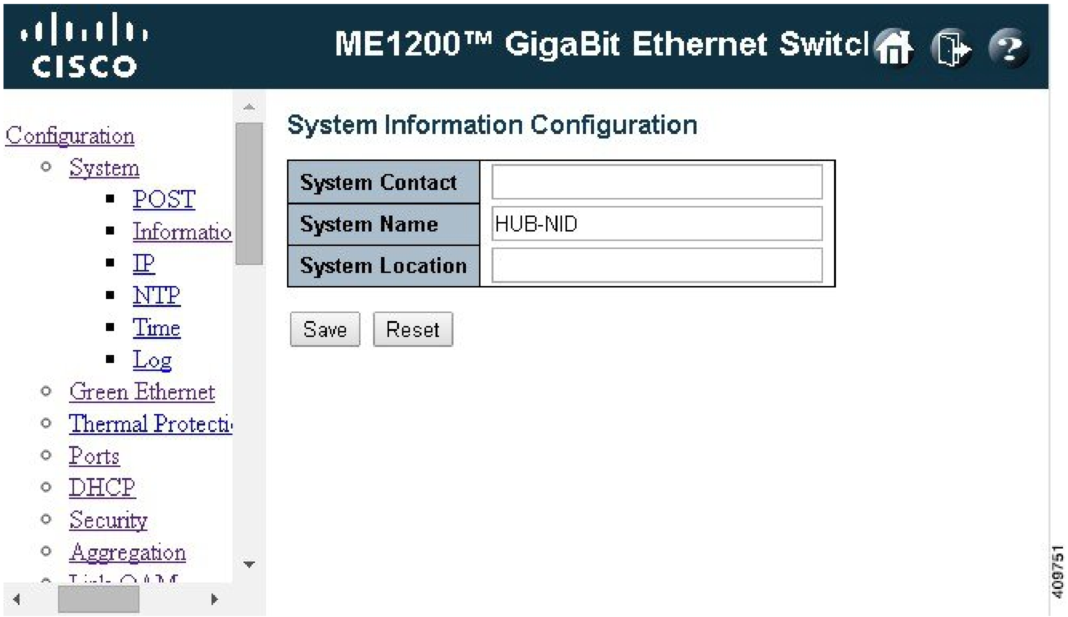
CHAPTER 2

Basic Configurations

This section describes the basic configurations that are available for the ME 1200 Web GUI interface.

Set Device Hostname and admin User Password

In the left panel, click **Configuration** > **System** > **Information**.

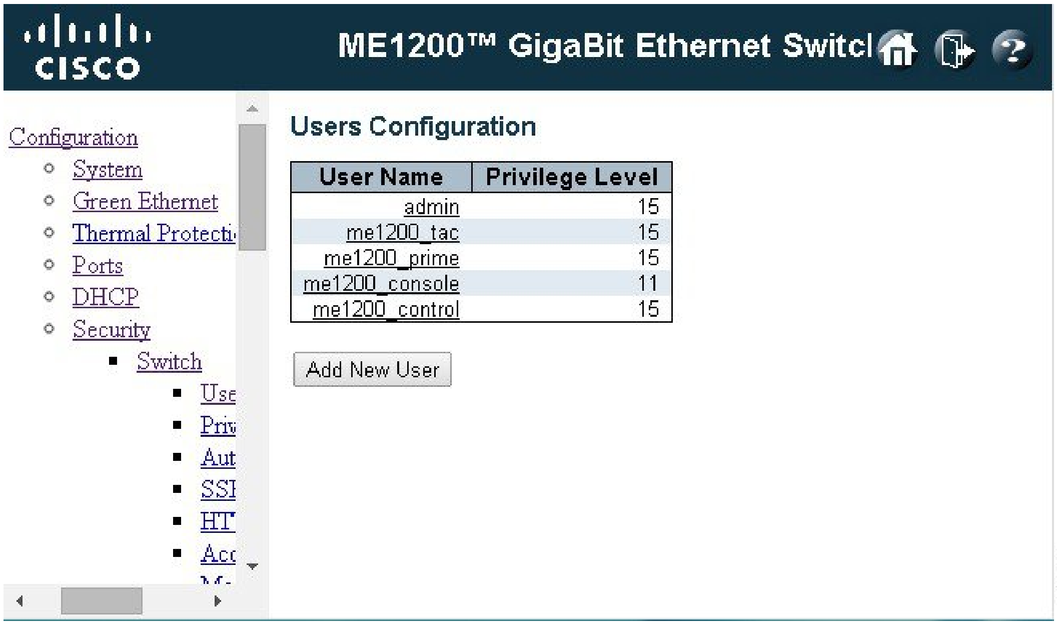


System Information Configuration

System Contact	
System Name	HUB-NID
System Location	

Enter the new hostname in the **System Name** box.

To change the password for a user, click **Configuration** > **Security** > **Switch** > **Users**.

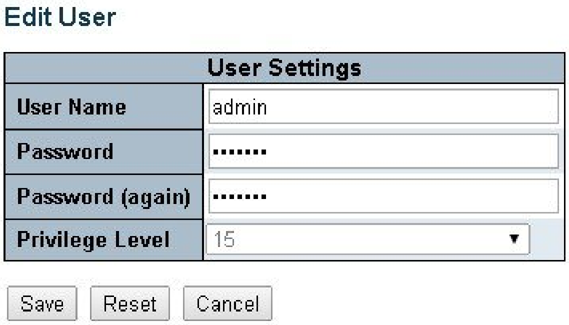


Users Configuration

User Name	Privilege Level
admin	15
me1200_tac	15
me1200_prime	15
me1200_console	11
me1200_control	15

409752

Click on the user whose password you wish to change, and enter the new password into the **Password** and **Password (again)** fields. Click **Save**.



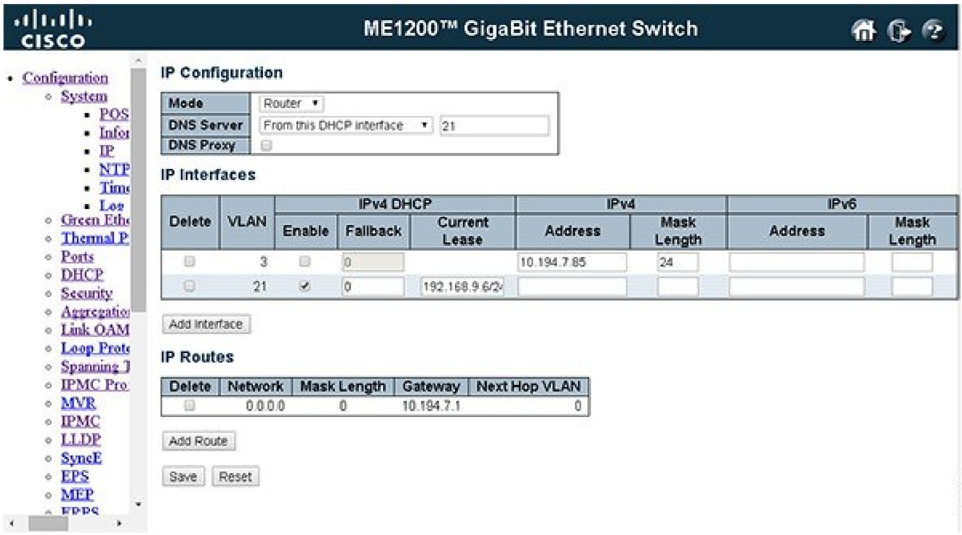
Edit User

User Settings	
User Name	admin
Password	•••••••
Password (again)	•••••••
Privilege Level	15 ▾

409753

Set VLAN IP Address

To set an address on a VLAN, first click **Configuration** > **System** > **IP**.



IP Configuration

Mode	Router
DNS Server	From this DHCP interface 21
DNS Proxy	□

IP Interfaces

Delete	VLAN	IPv4 DHCP			IPv4		IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Address	Mask Length
□	3	□	0		10.194.7.85	24		
□	21	☑	0	192.168.9.6/2				

Add Interface

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
□	0.0.0.0	0	10.194.7.1	0

Add Route

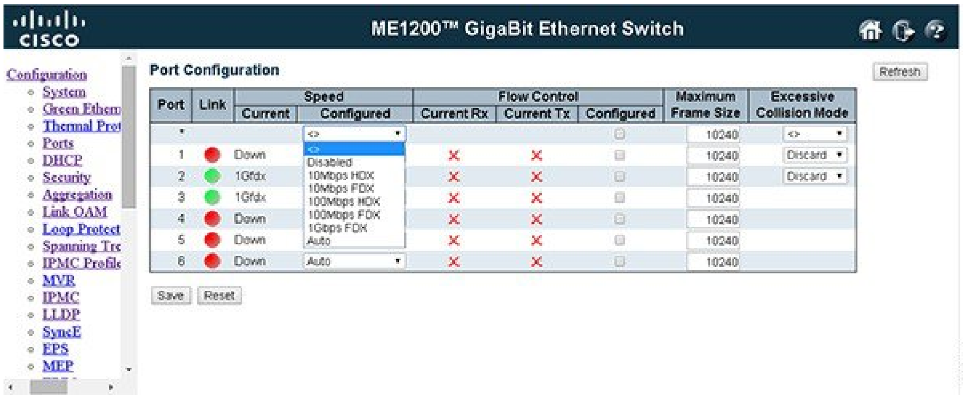
Save Reset

To create a new VLAN, click **Add interface**. To add an address or alter the address on an existing VLAN, simply type the new address into the appropriate text box along with the subnet mask.

Physical Port Configuration and Status

To configure ports:

1 To view and alter port configurations, click **Configuration** > **Ports**. Configure physical port parameters like enable/disable port, change MTU, and so on.

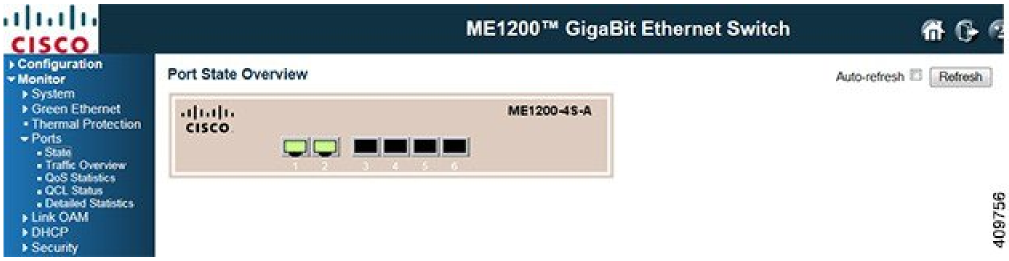


Port Configuration

Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode
		Current	Configured	Current Rx	Current Tx	Configured		
*			<>			□	10240	<>
1	●	Down		✗	✗	□	10240	Discard
2	●	1Gfdx		✗	✗	□	10240	Discard
3	●	1Gfdx		✗	✗	□	10240	
4	●	Down		✗	✗	□	10240	
5	●	Down		✗	✗	□	10240	
6	●	Down	Auto	✗	✗	□	10240	

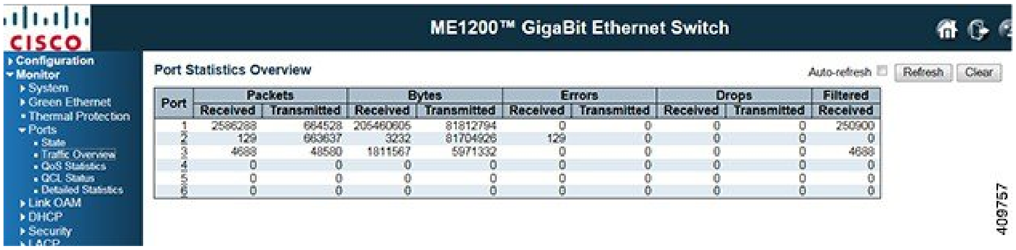
Save Reset

2 To monitor port status on the Chassis View, click **Monitor** > **Ports** > **State**.



Port State Overview

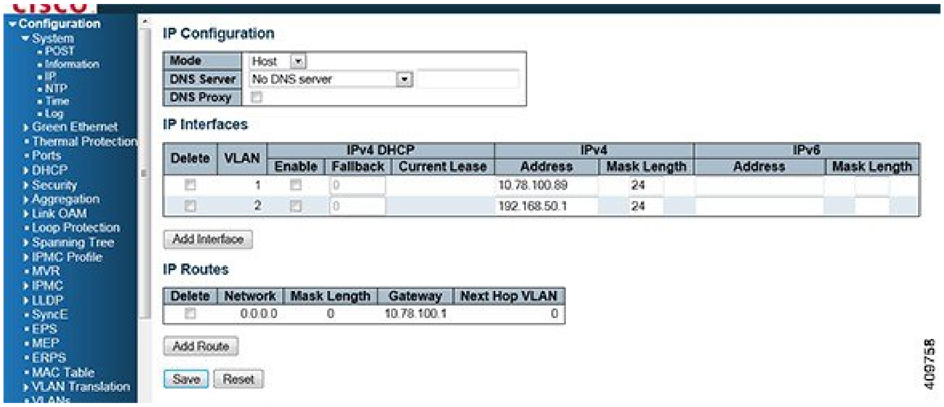
3 To monitor port statistics, click **Monitor** > **Ports** > **Traffic Overview**.



Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	2586288	664528	205460605	81812794	0	0	0	0	250900
2	129	663637	3232	81704926	129	0	0	0	0
3	4688	48580	1811567	5971332	0	0	0	0	4688
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0

4 To configure the management IP address on the ME 1200, click **Configuration** > **System** > **IP**.



IP Configuration

Mode	Host
DNS Server	No DNS server
DNS Proxy	□

IP Interfaces

Delete	VLAN	IPv4 DHCP			IPv4		IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Address	Mask Length
□	1	□	0		10.78.100.89	24		
□	2	□	0		192.168.50.1	24		

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
□	0.0.0.0	0	10.78.100.1	0

Related Topics

Configuring Ports, on page 33

Monitoring Ports, on page 181

L2 Switching

The IEEE 802.1Q standard VLANs are supported and the default configuration is as follows:

- All ports are VLAN aware.
- All ports are members of VLAN 1.

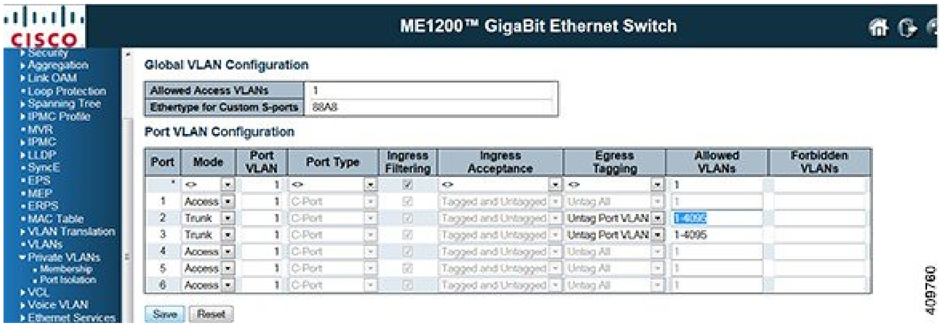
- The switch management interface is on VLAN 1.
- All ports have a Port VLAN ID (PVID) of 1.
- All ports can send and receive both VLAN-tagged and untagged packets.

In the default configuration, any port is able to send traffic to any other port, and a PC connected to any port will be able to reach the management interface. Broadcast traffic, for example, will be flooded to all ports on the switch.

Note 1 is always reserved for the default VLAN. The range of the VLAN ID is 2 to 4095.

Configuring VLAN for UNI and NNI Ports

Note It is recommended that you retain both ports as trunk ports with the range of all allowed VLANS.



Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	
3	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

For more information on configuring a private VLAN, see the *Configuring Private VLANs* section. .

Port Mode

The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below.

- **Access**

  Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:

  - Member of exactly one VLAN, the Port VLAN (also called as Access VLAN), which by default is 1, accepts untagged frames and C-tagged frames.
  - Discards all frames that are not classified to the Access VLAN.
  - On egress all frames are transmitted untagged.

- **Trunk**
  Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:

  - ◦ By default, a trunk port is member of all existing VLANs. This may be limited by the use of Allowed VLANs.
  - ◦ By default, all frames but frames classified to the Port VLAN (also called as Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress.
  - ◦ Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress.

- **Hybrid**

  Hybrid ports do resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:

  Port Type

  Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.

  Unaware: On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.

  C-Port: On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag.

  S-Port: On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.

  S-Custom-Port: On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.

Related Topics

Configuring VLANs, on page 97
Monitoring VLANs, on page 235

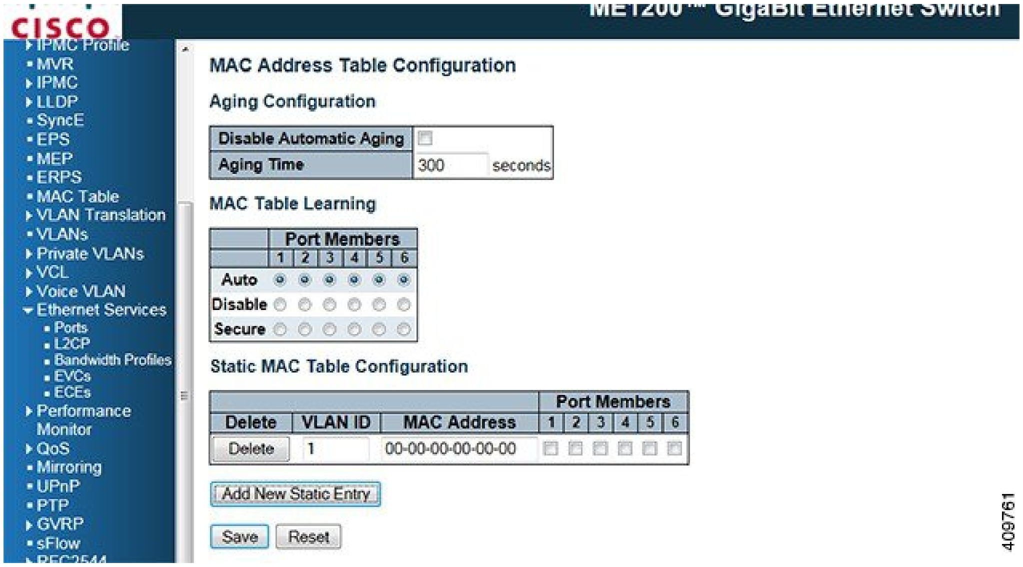
MAC Table Configuration

The following per port configuration parameters are available for MAC Learning configuration:

- Auto - Learning is done automatically as soon as a frame with unknown SMAC is received.
- Disable - No learning is done.
- Secure - Only static MAC entries are learned, all other frames are dropped.

The static entries can be configured in the MAC table for forwarding and the below parameters are allowed. The static MAC table can contain 64 entries.

To configure the MAC table, **Configuration** > **MAC Table**.



MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	□
Aging Time	300 seconds

MAC Table Learning

	Port Members					
	1	2	3	4	5	6
Auto	●	●	●	●	●	●
Disable	○	○	○	○	○	○
Secure	○	○	○	○	○	○

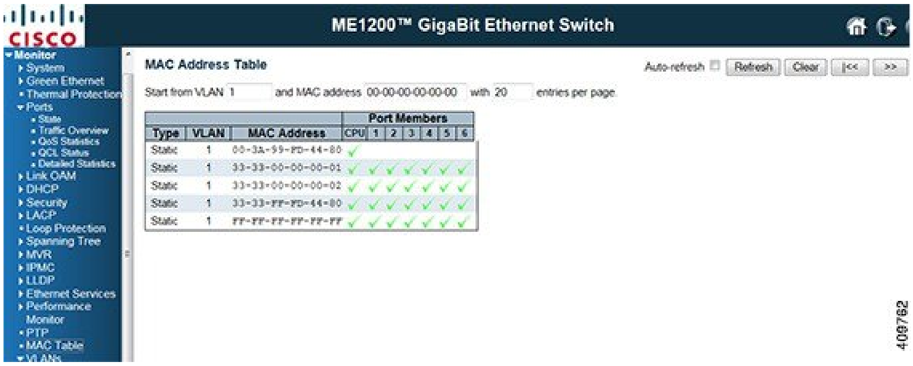
Static MAC Table Configuration

			Port Members					
Delete	VLAN ID	MAC Address	1	2	3	4	5	6
Delete	1	00-00-00-00-00-00	□	□	□	□	□	□

Add New Static Entry

Save Reset

To view the MAC table, **Monitor** > **MAC Table**.



MAC Address Table

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

			Port Members						
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6
Static	1	00-3A-99-FD-44-80	✓						
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-FD-44-80	✓	✓	✓	✓	✓	✓	✓
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓

Related Topics

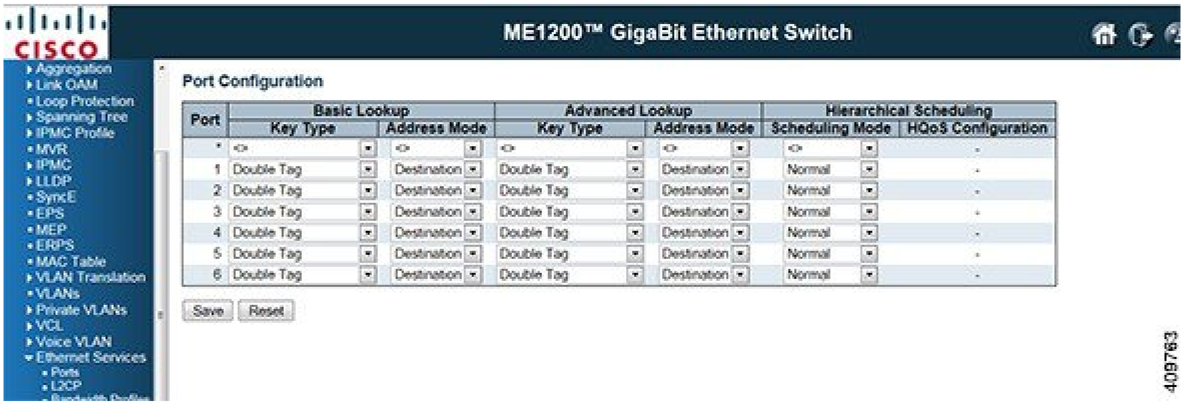
Configuring MAC Table, on page 95
Monitoring MAC Table, on page 233

Ethernet Services

MEF standards describe services provided to customers at User Network Interfaces (UNIs). Inside provider networks, nodes are connected using Internal Network-to-Network Interfaces (I-NNIs). Connections between service providers are done using External Network-to-Network Interfaces (E-NNIs). An Ethernet Virtual Connection (EVC) is an association of two or more UNIs.

Port Configuration

The EVC per Port configurations that are allowed are as shown below. Retain the default configuration for the MEF services.



Port Configuration

Port	Basic Lookup		Advanced Lookup		Hierarchical Scheduling	
	Key Type	Address Mode	Key Type	Address Mode	Scheduling Mode	HQoS Configuration
*	<>	<>	<>	<>	<>	-
1	Double Tag	Destination	Double Tag	Destination	Normal	-
2	Double Tag	Destination	Double Tag	Destination	Normal	-
3	Double Tag	Destination	Double Tag	Destination	Normal	-
4	Double Tag	Destination	Double Tag	Destination	Normal	-
5	Double Tag	Destination	Double Tag	Destination	Normal	-
6	Double Tag	Destination	Double Tag	Destination	Normal	-

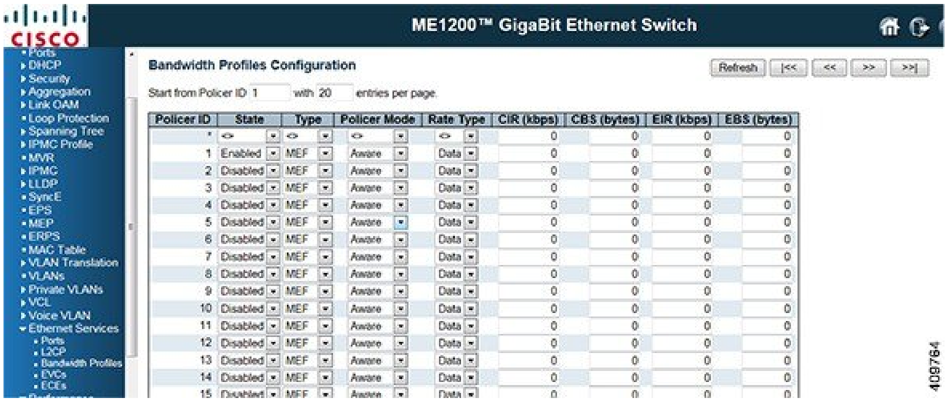
Related Topics

EVC Port Configuration, on page 103

Bandwidth Profiles Configuration

The EVC ingress bandwidth profile configurations are allowed as shown. These policers may be used to limit the traffic received on UNI ports.

Policer Mode	Coupled , Aware
CIR	0 to 10000000 kbps
CBS	0 to 100000 bytes
EIR	0 to 10000000 kbps
EBS	0 to 100000 bytes



Bandwidth Profiles Configuration

Start from Policer ID 1 with 20 entries per page.

Policer ID	State	Type	Policer Mode	Rate Type	CIR (kbps)	CBS (bytes)	EIR (kbps)	EBS (bytes)
*	<>	<>	<>	<>	0	0	0	0
1	Enabled	MEF	Aware	Data	0	0	0	0
2	Disabled	MEF	Aware	Data	0	0	0	0
3	Disabled	MEF	Aware	Data	0	0	0	0
4	Disabled	MEF	Aware	Data	0	0	0	0
5	Disabled	MEF	Aware	Data	0	0	0	0
6	Disabled	MEF	Aware	Data	0	0	0	0
7	Disabled	MEF	Aware	Data	0	0	0	0
8	Disabled	MEF	Aware	Data	0	0	0	0
9	Disabled	MEF	Aware	Data	0	0	0	0
10	Disabled	MEF	Aware	Data	0	0	0	0
11	Disabled	MEF	Aware	Data	0	0	0	0
12	Disabled	MEF	Aware	Data	0	0	0	0
13	Disabled	MEF	Aware	Data	0	0	0	0
14	Disabled	MEF	Aware	Data	0	0	0	0
15	Disabled	MEF	Aware	Data	0	0	0	0

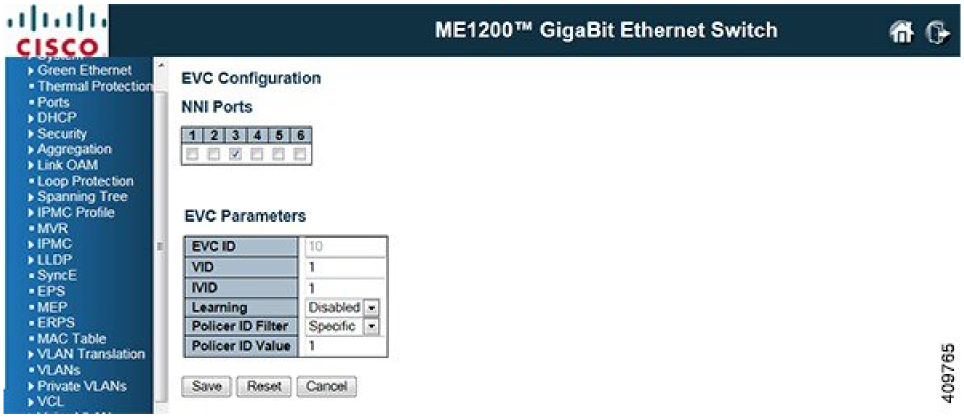
Related Topics

EVC Bandwidth Profile Configuration, on page 105

EVC

The EVC configurations that are allowed are as shown in the following table.

Configurable Parameter	Allowed Range
NNI Port	Any port number of the switch
EVC ID	1 to 128
VLAN ID	1 to 4095
Internal/ Classified VLAN ID	1 to 4095



EVC Configuration

NNI Ports

1	2	3	4	5	6
☐	☐	☑	☐	☐	☐

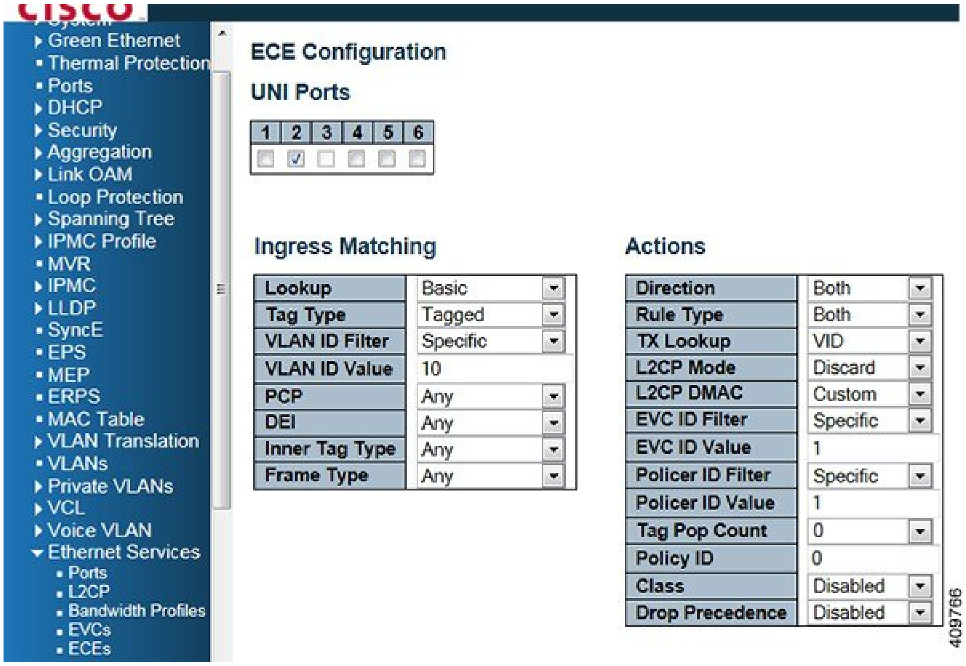
EVC Parameters

EVC ID	10
VID	1
IVID	1
Learning	Disabled
Policer ID Filter	Specific
Policer ID Value	1

ECE

The EVC Control Entry configurations that are allowed are as shown below.

These parameters vary according to the Tag type selected. The User Network Interface (UNI) port(s) needs to be selected for the ECE, and then the Tag type. Different parameter options are displayed depending on the Tag type selected.



ECE Configuration

UNI Ports

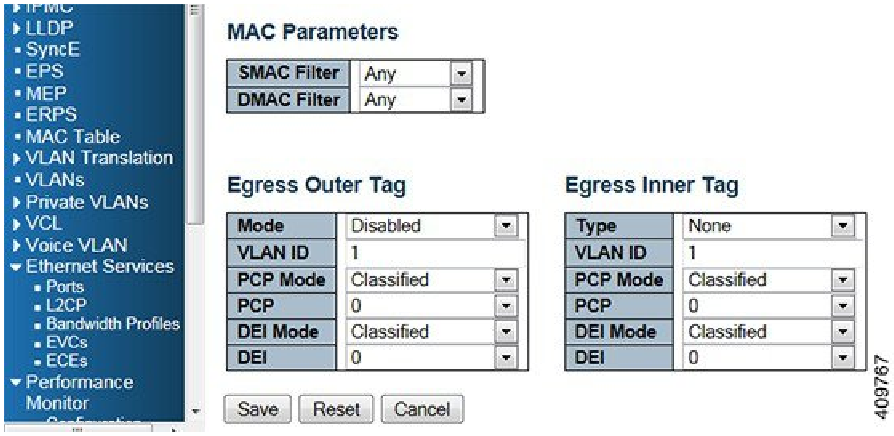
1	2	3	4	5	6
□	☑	□	□	□	□

Ingress Matching

Lookup	Basic
Tag Type	Tagged
VLAN ID Filter	Specific
VLAN ID Value	10
PCP	Any
DEI	Any
Inner Tag Type	Any
Frame Type	Any

Actions

Direction	Both
Rule Type	Both
TX Lookup	VID
L2CP Mode	Discard
L2CP DMAC	Custom
EVC ID Filter	Specific
EVC ID Value	1
Policer ID Filter	Specific
Policer ID Value	1
Tag Pop Count	0
Policy ID	0
Class	Disabled
Drop Precedence	Disabled



MAC Parameters

SMAC Filter	Any
DMAC Filter	Any

Egress Outer Tag

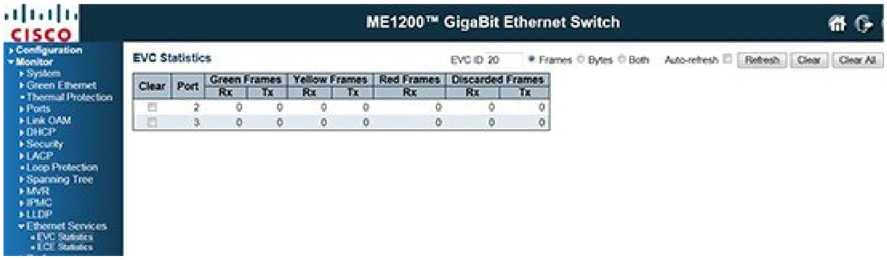
Mode	Disabled
VLAN ID	1
PCP Mode	Classified
PCP	0
DEI Mode	Classified
DEI	0

Egress Inner Tag

Type	None
VLAN ID	1
PCP Mode	Classified
PCP	0
DEI Mode	Classified
DEI	0

For details of each parameter, refer to the Help section on the GUI. The EVC/ECE Service statistics can be viewed via the Monitor pages.

EVC Statistics

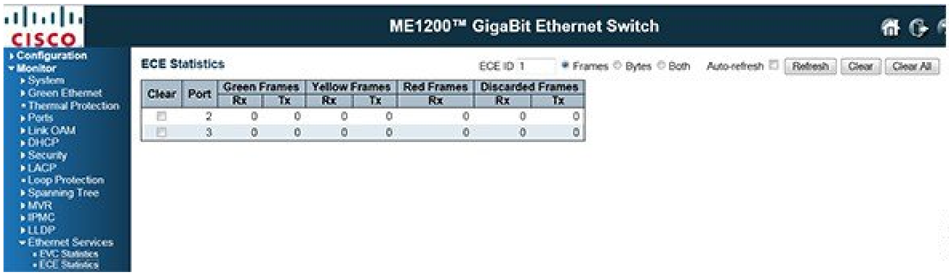


EVC Statistics

EVC ID 20 ● Frames ○ Bytes ○ Both Auto-refresh □

Clear	Port	Green Frames		Yellow Frames		Red Frames	Discarded Frames	
		Rx	Tx	Rx	Tx	Rx	Rx	Tx
□	2	0	0	0	0	0	0	0
□	3	0	0	0	0	0	0	0

ECE Statistics



ECE Statistics

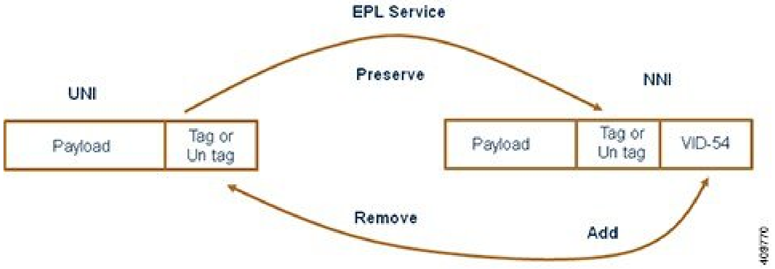
ECE ID 1 ● Frames ○ Bytes ○ Both Auto-refresh □

Clear	Port	Green Frames		Yellow Frames		Red Frames	Discarded Frames	
		Rx	Tx	Rx	Tx	Rx	Rx	Tx
□	2	0	0	0	0	0	0	0
□	3	0	0	0	0	0	0	0

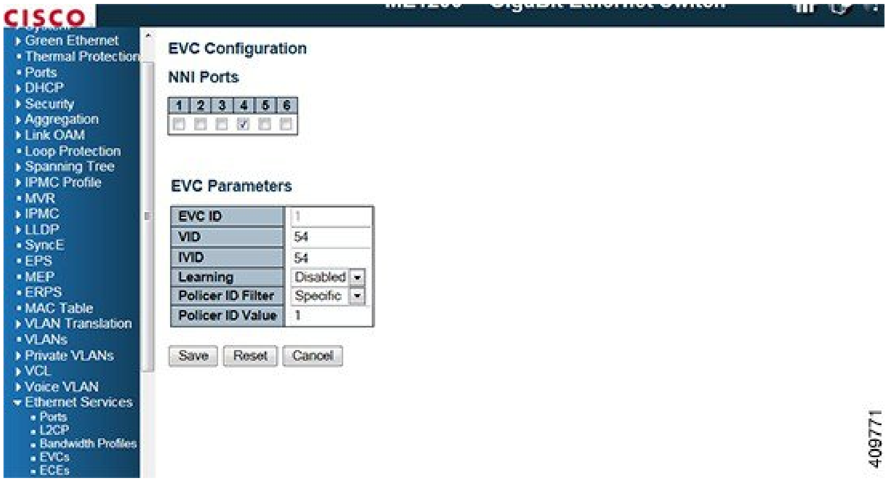
EPL Service between UNI and NNI

To set up an EPL service between UNI and NNI:

- Set up an EPL service (all to one bundling) on a UNI (port 1).
- On NNI (port 4) egress, add a tag (54).
- On UNI egress, pop or remove the tag.



First, create EVC as shown below. VID is 54, for IVID, that is, the internal VID used for internal classification is also set to 54, but any unique value can be used. Learning is disabled because this is a point to point service and the NNI port is 4. Double VLAN tagging on the NNI is not used, so no inner tag is specified. The Outer Tag VID used for uni-directional NNI to UNI service and is not used here.



EVC Configuration

NNI Ports

1	2	3	4	5	6
□	□	□	☑	□	□

EVC Parameters

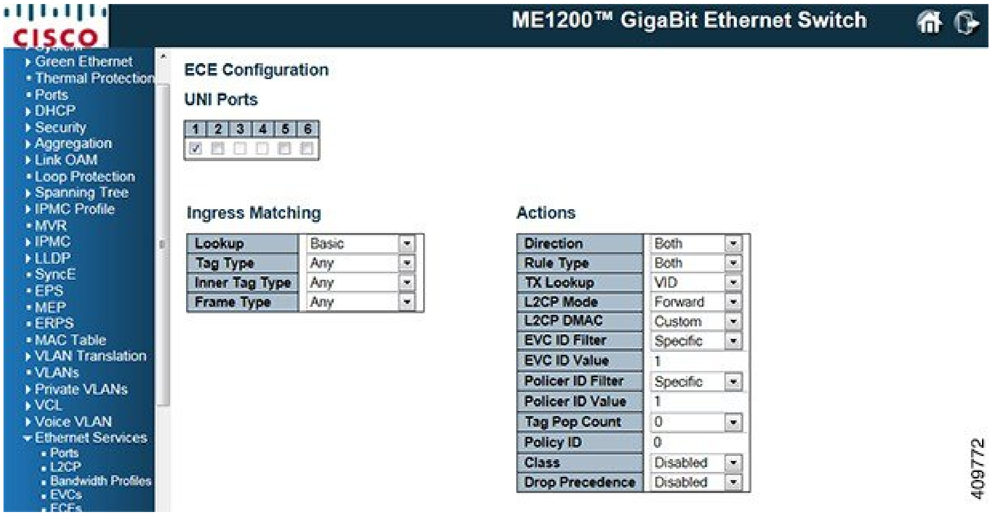
EVC ID	1
VID	54
IVID	54
Learning	Disabled
Policer ID Filter	Specific
Policer ID Value	1

Then, create EVC Control Entry (ECE). The ECE controls the UNI configuration. The following parameters are used for this service:

- UNI port is port 1.
- UNI matching is any for all to one bundling.
- MAC parameters are set to any.
- NNI outer tag allows inserting a tag on the UNI. This is for unidirectional services only.

  Actions: EVC ID is 1.

  - Direction is both equal to a bidirectional service.
  - Tag Pop Count is 0 for EPL service, that is, all frames are passed to the EVC without popping any tags.
  - The policy ID is used to point to an ACL. The ACL can then be used to select an EVC policer. This service is not using any policer, policy ID 0 is used.



ECE Configuration

UNI Ports

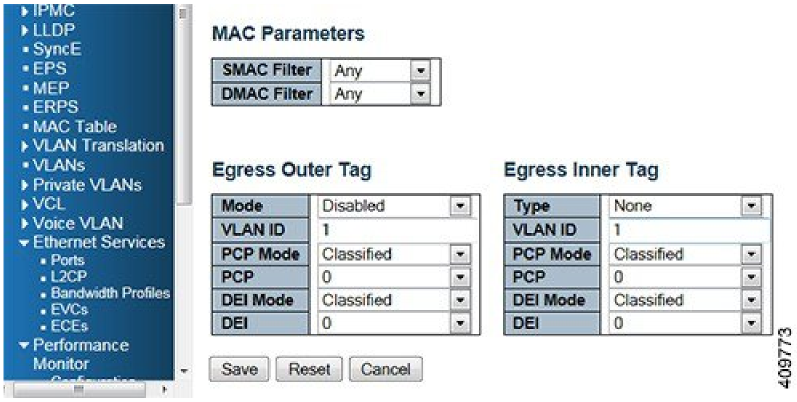
1	2	3	4	5	6
☑	□	□	□	□	□

Ingress Matching

Lookup	Basic
Tag Type	Any
Inner Tag Type	Any
Frame Type	Any

Actions

Direction	Both
Rule Type	Both
TX Lookup	VID
L2CP Mode	Forward
L2CP DMAC	Custom
EVC ID Filter	Specific
EVC ID Value	1
Policer ID Filter	Specific
Policer ID Value	1
Tag Pop Count	0
Policy ID	0
Class	Disabled
Drop Precedence	Disabled



MAC Parameters

SMAC Filter	Any
DMAC Filter	Any

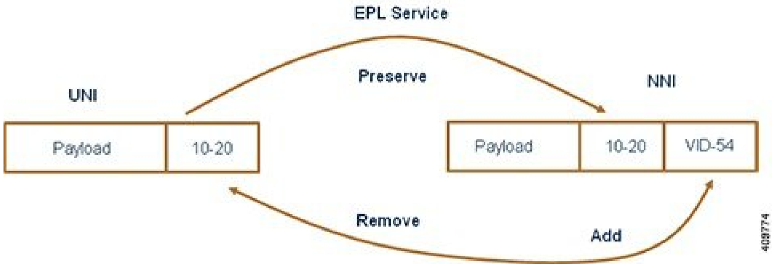
Egress Outer Tag

Mode	Disabled
VLAN ID	1
PCP Mode	Classified
PCP	0
DEI Mode	Classified
DEI	0

Egress Inner Tag

Type	None
VLAN ID	1
PCP Mode	Classified
PCP	0
DEI Mode	Classified
DEI	0

EVPL Service between UNI and NNI (bundle #1)



Set up an EVPL service (bundling) on a UNI (port 2) for CEVLAN IDs 10-20.

- On NNI (port 4) egress, add a tag 54.
- On UNI egress, pop or remove the tag.

EVC configuration is the same as the first example.

ECE Configuration

Create ECE (EVC Control Entry)

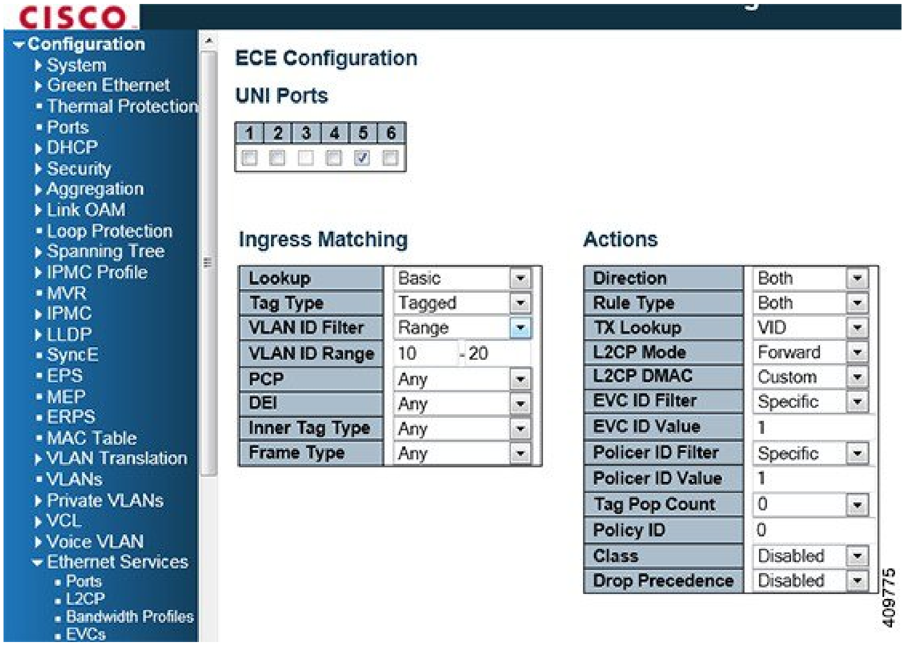
The following parameters are used for this service:

- UNI port is port 2.
- Uni Matching VID 10-20.
- MAC parameters are set to any.
- NNI outer tag allows to insert a tag on the UNI. This is for uni-directional services only, and is not used here.

Actions: EVC ID is 2.

- Direction is both equal to a bidirectional service.

- Tag Pop Count is 0 for EVPL service, that is, all frames are passed to the EVC without popping any tags. The UNI tag is preserved.
- The policy ID is used to point to an ACL. The ACL can then be used to select an EVC policer. This service is not using any policer, policy ID 0 is used.



ECE Configuration

UNI Ports

1	2	3	4	5	6
☐	☐	☐	☐	☑	☐

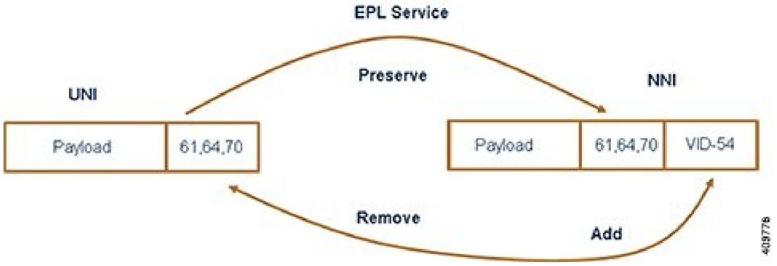
Ingress Matching

Lookup	Basic
Tag Type	Tagged
VLAN ID Filter	Range
VLAN ID Range	10 - 20
PCP	Any
DEI	Any
Inner Tag Type	Any
Frame Type	Any

Actions

Direction	Both
Rule Type	Both
TX Lookup	VID
L2CP Mode	Forward
L2CP DMAC	Custom
EVC ID Filter	Specific
EVC ID Value	1
Policer ID Filter	Specific
Policer ID Value	1
Tag Pop Count	0
Policy ID	0
Class	Disabled
Drop Precedence	Disabled

EVPL service between UNI and NNI (bundle #2), same UNI, NNI as above



Set up an EVPL service (bundling) on a UNI (port 2) for CEVLAN IDs 61, 64, 70.

- On NNI (port 4) egress, add a tag 54.
- On UNI egress, pop or remove the tag.

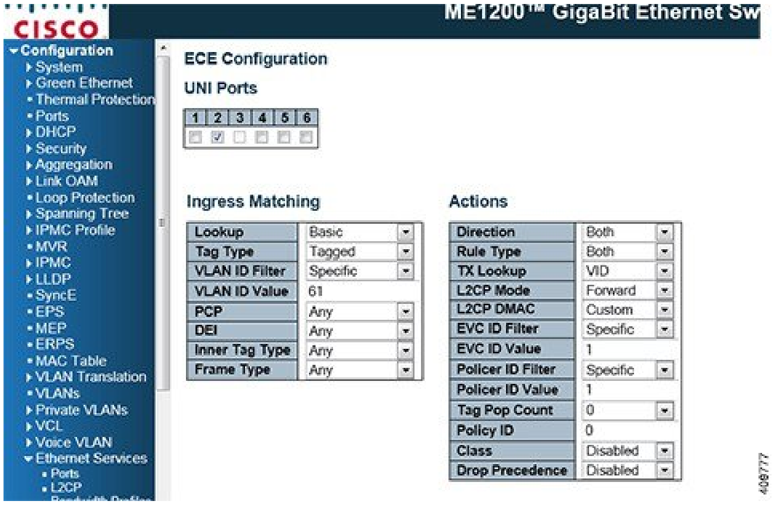
First, create EVC as shown in figure. VID is 54, Inner VID is 54. Learning is disabled because this is a point-to-point service and the NNI port is 4. Then, create ECE (EVC Control Entry).

The following parameters are used for this service:

- UNI port is port 2.
- UNI Matching VID 61.
- MAC parameters are set to any.
- NNI outer tag allows to insert a tag on the UNI. This is for unidirectional services only, and is not used here.

Actions: EVC ID is 3.

- Direction is both equal to a bidirectional service.
- Tag Pop Count is 0 for EVPL service, that is, all frames are passed to the EVC without popping any tags. The UNI tag is preserved.
- The policy ID is used to point to an ACL. The ACL can then be used to select an EVC policer. This service is not using any policer, policy ID 0 is used.



ECE Configuration

UNI Ports

1	2	3	4	5	6
□	☑	□	□	□	□

Ingress Matching

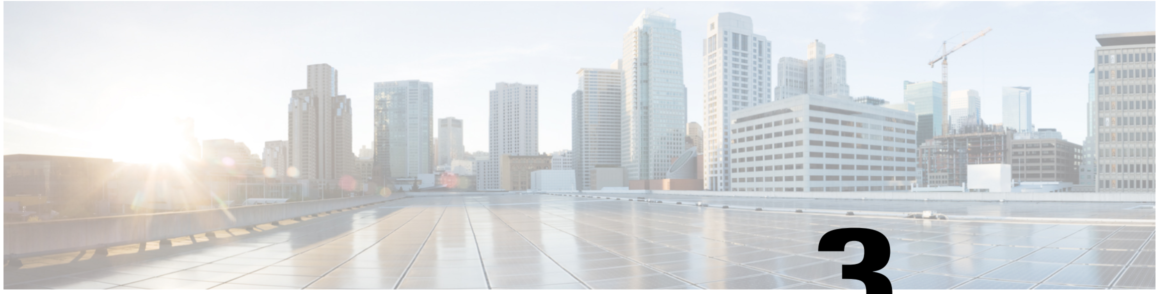
Lookup	Basic
Tag Type	Tagged
VLAN ID Filter	Specific
VLAN ID Value	61
PCP	Any
DEI	Any
Inner Tag Type	Any
Frame Type	Any

Actions

Direction	Both
Rule Type	Both
TX Lookup	VID
L2CP Mode	Forward
L2CP DMAC	Custom
EVC ID Filter	Specific
EVC ID Value	1
Policer ID Filter	Specific
Policer ID Value	1
Tag Pop Count	0
Policy ID	0
Class	Disabled
Drop Precedence	Disabled

Create similar ECE for 64 and 70 with the same EVC ID.

EVPL service between UNI and NNI (bundle #2), same UNI, NNI as above



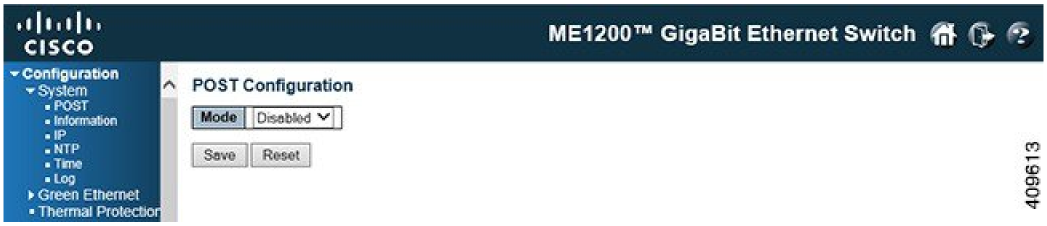
CHAPTER 3

Configuring System

The System feature available on the ME 1200 Web GUI allows you to view and reset your computer's configuration information.

POST Configuration

This option allows you to set the POST configuration.



POST Configuration

Mode: Disabled

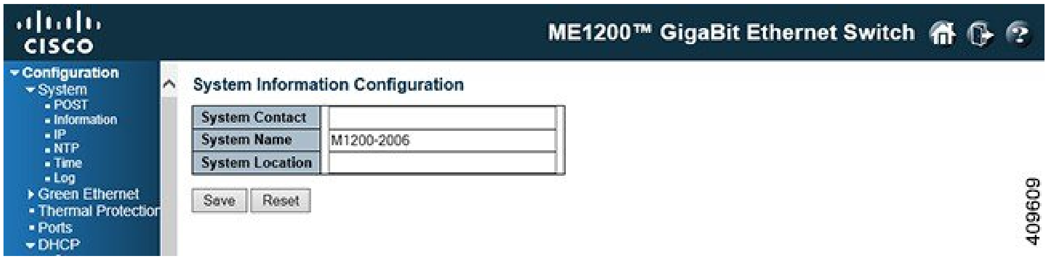
Mode

Mode Indicates the POST mode operation. Possible modes are:

- *Enabled*: Enables POST mode operation.
- *Disabled*: Disables POST mode operation.

System Information Configuration

This option allows you to configure the system information for the switch.



System Information Configuration

System Contact	
System Name	M1200-2006
System Location	

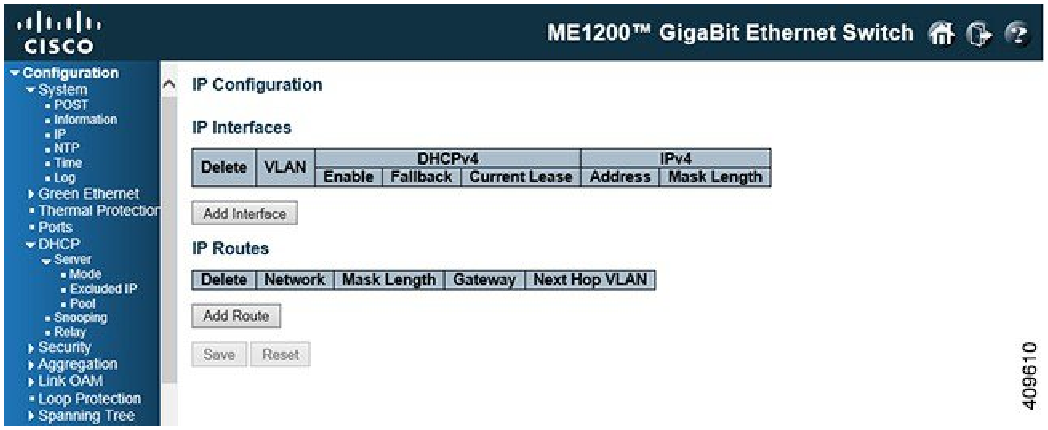
- **System Contact**: The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
- **System Name**: An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
- **System Location**: The physical location of this node(for example, telephone closet, third floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

Related Topics

Monitoring System, on page 169

IP Configuration

This option allows you to configure IP basic settings, control IP interfaces, and IP routes.



IP Configuration

IP Interfaces

Delete	VLAN	DHCPv4			IPv4	
		Enable	Fallback	Current Lease	Address	Mask Length

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN

The maximum number of interfaces supported is 128 and the maximum number of routes is 32.

Basic Settings

- **Mode**: Configure whether the IP stack should act as a *Host* or a *Router*. In *Host* mode, IP traffic between interfaces will not be routed. In *Router* mode traffic is routed between all interfaces.
- **DNS Server**: This setting controls the DNS name resolution done by the switch. There are four servers available for configuration, and the index of the server presents the preference (less index has higher priority) in doing DNS name resolution. System selects the active DNS server from configuration in turn, if the preferred server does not respond in five attempts. The following modes are supported:
    - **From any DHCPv4 interfaces**: The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used.
    - **No DNS server**: No DNS server will be used
    - **Configured IPv4**: Explicitly provide the valid IPv4 unicast address of the DNS Server in dotted decimal notation.

      Make sure the configured DNS server could be reachable (for example, via PING) for activating DNS service.
    - **From this DHCPv4 interface**: Specify from which DHCPv4-enabled interface a provided DNS server should be preferred.
    - **Configured IPv6**: Explicitly provide the valid IPv6 unicast (except linklocal) address of the DNS Server.

      Make sure the configured DNS server could be reachable (for example, via PING6) for activating DNS service.
    - **From this DHCPv6 interface**: Specify from which DHCPv6-enabled interface a provided DNS server should be preferred.
    - **From any DHCPv6 interfaces**: The first DNS server offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used.
    - **DNS Proxy**: When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network.

      Only IPv4 DNS proxy is now supported.
- **IP Interfaces**
    - **Delete**: Select this option to delete an existing IP interface.
    - **VLAN**: The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.
    - **IPv4 DHCP Enabled**: Enable the DHCPv4 client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol. The DHCPv4 client will announce the configured System Name as hostname to provide DNS lookup.
    - **IPv4 DHCP Fallback Timeout**: The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.

- **IPv4 DHCP Current Lease**: For DHCP interfaces with an active lease, this column show the current interface address, as provided by the DHCP server.
- IPv4 Address: The IPv4 address of the interface in dotted decimal notation.

  If DHCP is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.
- **IPv4 Mask**: The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for an IPv4 address.

  If DHCP is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.
- **DHCPv6 Enable**: Enable the DHCPv6 client by checking this box. If this option is enabled, the system will configure the IPv6 address of the interface using the DHCPv6 protocol.
- **DHCPv6 Rapid Commit**: Enable the DHCPv6 Rapid-Commit option by checking this box. If this option is enabled, the DHCPv6 client terminates the waiting process as soon as a Reply message with a Rapid Commit option is received.

  This option is only manageable when DHCPv6 client is enabled.
- **DHCPv6 Current Lease**: For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server.
- **IPv6 Address**: The IPv6 address of the interface. An IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once.

  System accepts the valid IPv6 unicast address only, except IPv4-Compatible address and IPv4-Mapped address.

  The field may be left blank if IPv6 operation on the interface is not desired.
- **IPv6 Mask**: The IPv6 network mask, in number of bits (prefix length). Valid values are between 1 and 128 bits for an IPv6 address.

  The field may be left blank if IPv6 operation on the interface is not desired.
- **Resolving IPv6 DAD**: The link-local address is formed from an interface identifier based on the hardware address which is supposed to be uniquely assigned. Once the Duplicate Address Detection (DAD) detects the address duplication, the operation on the interface SHOULD be disabled.

  At this moment, manual intervention is required to resolve the address duplication. For example, check whether the loop occurs in the VLAN or there is indeed other device occupying the same hardware address as the device in the VLAN.

  After making sure the specific link-local address is unique on the IPv6 link in use, delete and then add the specific IPv6 interface to restart the IPv6 operations on this interface.

IP Routes

- **Delete:** Select this option to delete an existing IP route.
- **Network**: The destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0or IPv6 :: notation.

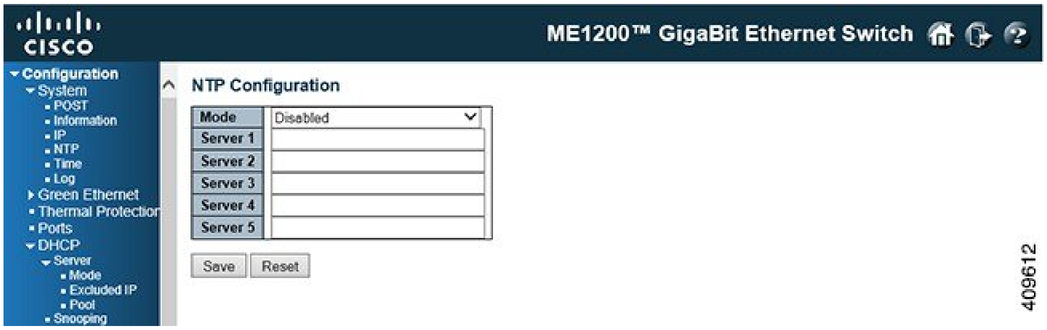
- **Mask Length**: The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).
- **Gateway**: The IP address of the IP gateway. Valid format is dotted decimal notationor a valid IPv6 notation. Gateway and Network must be of the same type.
- **Next Hop VLAN (Only for IPv6)**: The VLAN ID (VID) of the specific IPv6 interface associated with the gateway. The given VID ranges from 1 to 4095 and will be effective only when the corresponding IPv6 interface is valid.
    - If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway.
    - If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.

Related Topics

Monitoring System, on page 169

NTP Configuration

This option allows you to configure NTP.



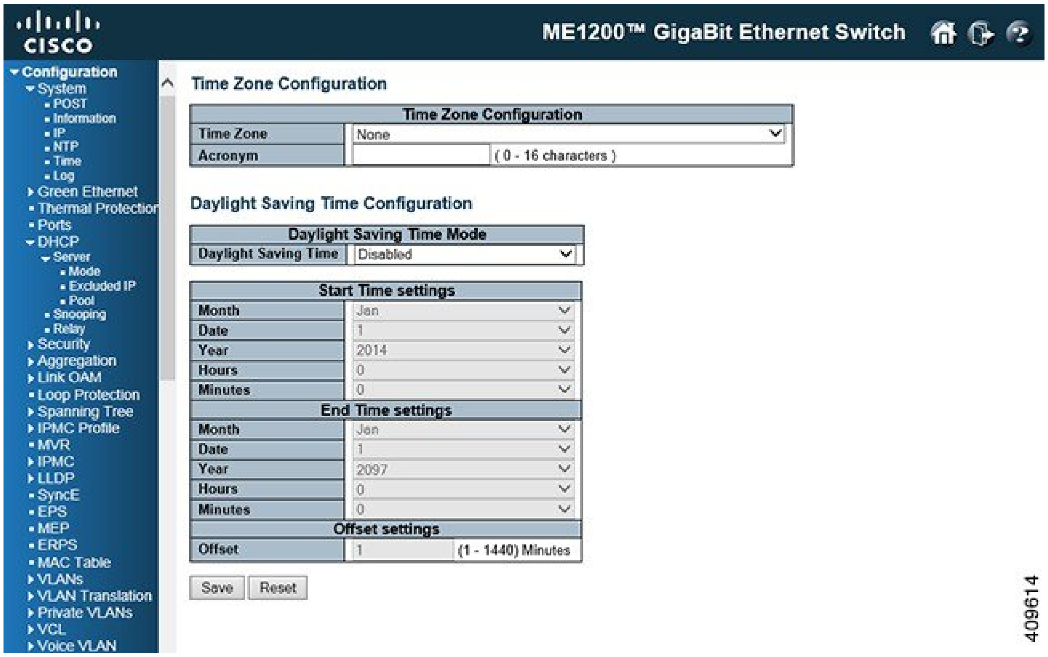
NTP Configuration

Mode	Disabled
Server 1	
Server 2	
Server 3	
Server 4	
Server 5	

- **Mode**: Indicates the NTP mode operation. Possible modes are:
    - *Enabled*: Enable NTP client mode operation.
    - *Disabled*: Disable NTP client mode operation.
- **Server #**: Provide the IPv4 or IPv6 address of a NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, `fe80::215:c5ff:fe03:4dc7`. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, `'::192.1.2.34'`. In addition, it can also accept a domain name address.

Time Zone Configuration

This option allows you to configure the Time Zone.



Time Zone Configuration

Time Zone Configuration	
Time Zone	None
Acronym	(0 - 16 characters)

Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Disabled

Start Time settings	
Month	Jan
Date	1
Year	2014
Hours	0
Minutes	0
End Time settings	
Month	Jan
Date	1
Year	2097
Hours	0
Minutes	0
Offset settings	
Offset	1 (1 - 1440) Minutes

- **Time Zone**: Lists the various Time Zones world wide. Select appropriate Time Zone from the drop down and click **Save** to set.
- **Acronym**: User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range : Up to 16 characters).
- **Daylight Saving Time Configuration**: This option is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select **Disable** to disable the Daylight Saving Time configuration. Select **Recurring** and configure the Daylight Saving Time duration to repeat the configuration every year. Select **Non-Recurring** and configure the Daylight Saving Time duration for single time configuration. (Default : Disabled)

Recurring Configurations

Start time settings	• **Week** - Select the starting week number. • **Day** - Select the starting day. • **Month** - Select the starting month. • **Hours** - Select the starting hour. • **Minutes** - Select the starting minute.

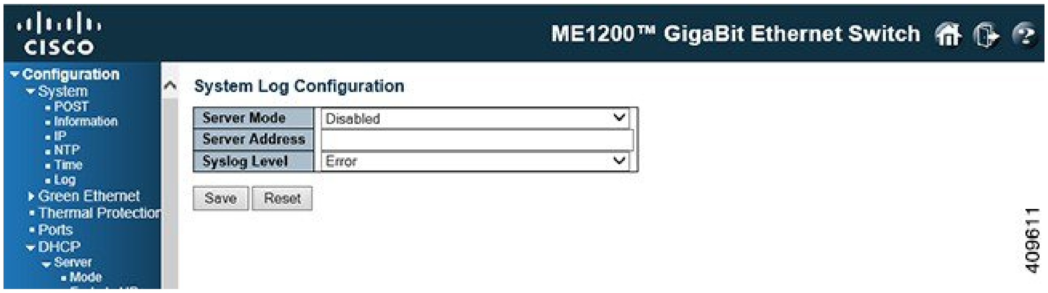
End time settings	• **Week** - Select the ending week number. • **Day** - Select the ending day. • **Month** - Select the ending month. • **Hours** - Select the ending hour. • **Minutes** - Select the ending minute.
Offset settings	Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

Non-Recurring Configurations

Start time settings	• **Month** - Select the starting month. • **Date** - Select the starting date. • **Year** - Select the starting year. • **Hours** - Select the starting hour. • **Minutes** - Select the starting minute.
End time settings	• **Month** - Select the ending month. • **Date** - Select the ending date. • **Year** - Select the ending year. • **Hours** - Select the ending hour. • **Minutes** - Select the ending minute.
Offset settings	Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

System Log Configuration

This option allows you to configure the System Log.



System Log Configuration

Server Mode	Disabled
Server Address	
Syslog Level	Error

- **Server Mode**: Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to the syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are:
  - *Enabled*: Enable server mode operation.
  - *Disabled*: Disable server mode operation.
- **Server Address**: Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a domain name.
- **Syslog Level**: Indicates what kind of message will send to syslog server. Possible modes are:
  - *Error* : Send the specific messages which severity code is less or equal than Error (3).
  - *Warning*: Send the specific messages which severity code is less or equal than Warning (4).
  - *Notice*: Send the specific messages which severity code is less or equal than Notice (5).
  - *Informational*: Send the specific messages which severity code is less or equal than Informational (6).

Related Topics

Monitoring System, on page 169

CHAPTER 4

Configuring Green Ethernet

The Green Ethernet feature available on the ME 1200 Web GUI allows you to set the port power savings configuration.

Port Power Savings Configuration

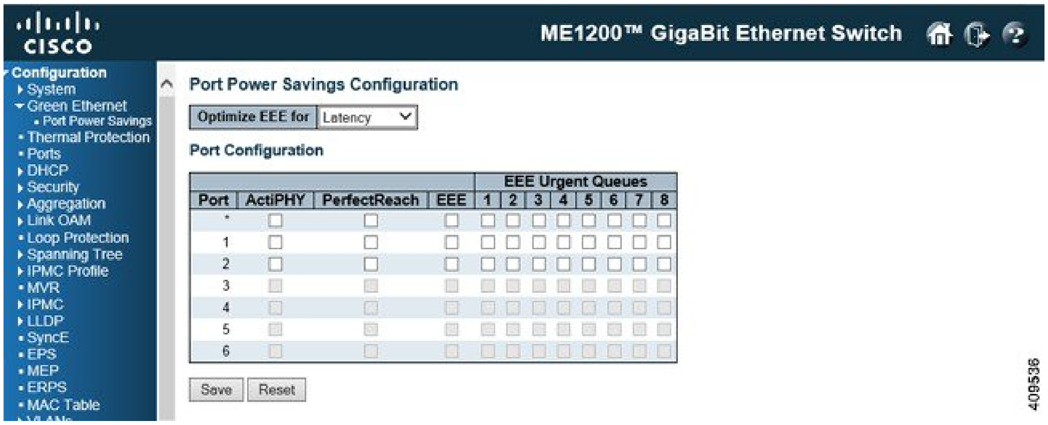
EEE is a power saving option that reduces the power usage when there is low or no traffic utilization.

EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted, all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 microseconds for 1 Gbit links and 30 microseconds for other link speeds. EEE devices must agree upon the value of the wakeup time to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP protocol.

EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1 G or 100 Mbit full duplex mode.

For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE for.

When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there are some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic.



Port Power Savings Configuration

Optimize EEE for: Latency

Port Configuration

				EEE Urgent Queues							
Port	ActiPHY	PerfectReach	EEE	1	2	3	4	5	6	7	8
*	□	□	□	□	□	□	□	□	□	□	□
1	□	□	□	□	□	□	□	□	□	□	□
2	□	□	□	□	□	□	□	□	□	□	□
3	□	□	□	□	□	□	□	□	□	□	□
4	□	□	□	□	□	□	□	□	□	□	□
5	□	□	□	□	□	□	□	□	□	□	□
6	□	□	□	□	□	□	□	□	□	□	□

Use the **Optimize EEE for** option to optimize EEE for either best power saving or least traffic latency.

The following options are available for **Port Configuration**:

- **Port**: The switch port number of the logical port.
- **ActiPHY**: Link down power savings enabled. ActiPHY works by lowering the power for a port when there is no link. The port is power up for short moment in order to determine if cable is inserted.
- **PerfectReach**: Cable length power savings enabled. PerfectReach works by determining the cable length and lowering the power for ports with short cables.
- **EEE**: Controls whether EEE is enabled for this switch port. For maximizing power savings, the circuit is not started at once transmit data is ready for a port, but is instead queued until a burst of data is ready to be transmitted. This will give some traffic latency.

  If desired, it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.
- **EEE Urgent Queues**: Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

Related Topics

Monitoring Green Ethernet, on page 177

CHAPTER 5

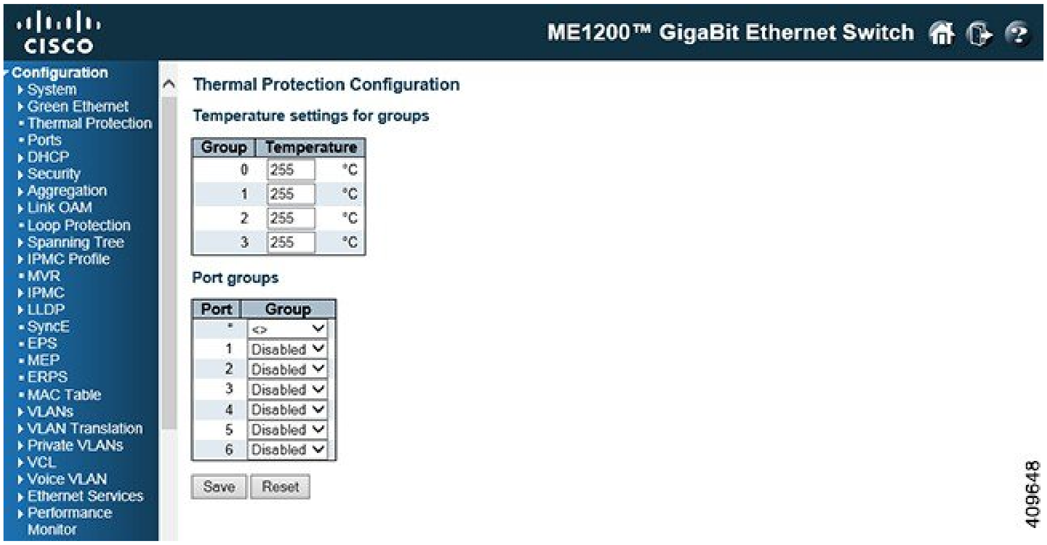
Configuring Thermal Protection

The Thermal Protection feature available on the ME 1200 Web GUI allows you to configure the Thermal Protection for the ME 1200 switch.

Thermal Protection Configuration

This option allows the user to inspect and configure the current setting for controlling thermal protection. Thermal protection is used to protect the chip from getting overheated.

When the temperature exceeds the configured thermal protection temperature, ports will be turned off in order to decrease the power consumption. It is possible to arrange the ports with different groups. Each group can be given a temperature at which the corresponding ports shall be turned off.



Thermal Protection Configuration

Temperature settings for groups

Group	Temperature	
0	255	°C
1	255	°C
2	255	°C
3	255	°C

Port groups

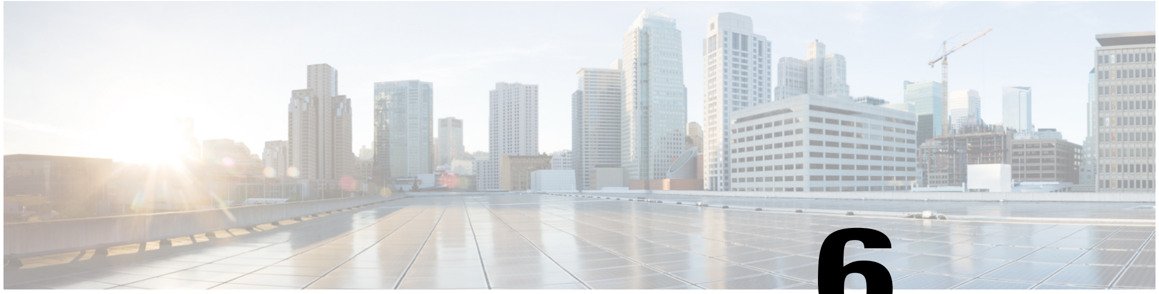
Port	Group
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled

- **Temperature settings for groups**: Temperature settings for groups. The temperature at which the ports with the corresponding group will be turned off. Temperatures between 0 and 255 C are supported.

- **Port groups**: The group the port belongs to. 4 groups are supported.

Related Topics

Monitoring Thermal Protection, on page 179

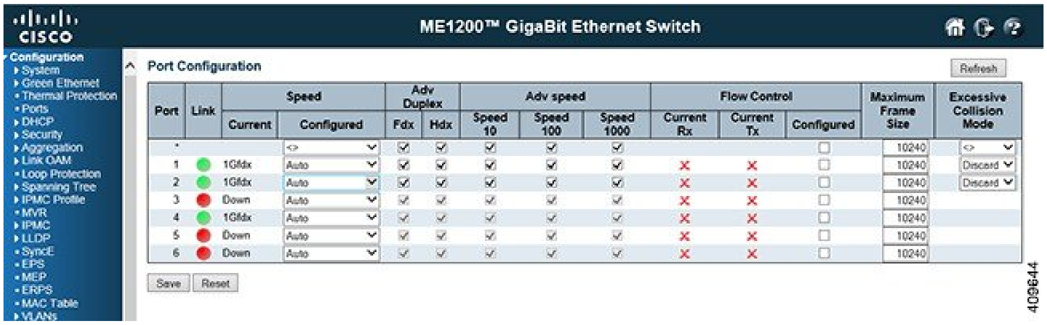


CHAPTER 6

Configuring Ports

Port Configuration

This feature displays current port configurations. Ports can also be configured using this feature.



Port Configuration

Port	Link	Speed		Adv Duplex		Adv speed			Flow Control			Maximum Frame Size	Excessive Collision Mode
		Current	Configured	Fdx	Hdx	Speed 10	Speed 100	Speed 1000	Current Rx	Current Tx	Configured		
*			<>	☑	☑	☑	☑	☑			☐	10240	<>
1	🟢	1Gfdx	Auto	☑	☑	☑	☑	☑	✗	✗	☐	10240	Discard
2	🟢	1Gfdx	Auto	☑	☑	☑	☑	☑	✗	✗	☐	10240	Discard
3	🔴	Down	Auto	☑	☑	☑	☑	☑	✗	✗	☐	10240	
4	🟢	1Gfdx	Auto	☑	☑	☑	☑	☑	✗	✗	☐	10240	
5	🔴	Down	Auto	☑	☑	☑	☑	☑	✗	✗	☐	10240	
6	🔴	Down	Auto	☑	☑	☑	☑	☑	✗	✗	☐	10240	

- **Port**: This is the logical port number for this row.
- **Link**: The current link state is displayed graphically. Green indicates the link is up and red that it is down.
- **Current Link Speed**: Current Link Speed. Provides the current link speed of the port.
- **Configured Link Speed**: Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are:
    - *Disabled*: Disables the switch port operation.
    - *Auto*: Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner.
    - *10Mbps HDX*: Forces the cu port in 10 Mbps half duplex mode.
    - *10Mbps FDX* : Forces the cu port in 10 Mbps full duplex mode.
    - *100Mbps HDX*: Forces the cu port in 100 Mbps half duplex mode.

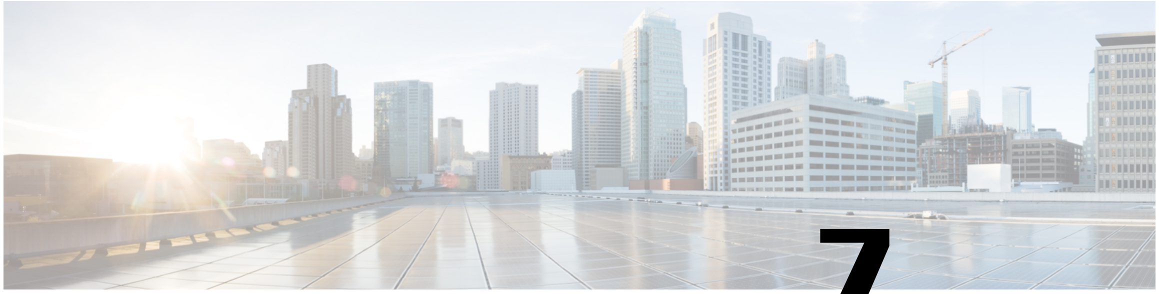
  - *100Mbps FDX*: Forces the cu port in 100 Mbps full duplex mode.
  - *1Gbps FDX*: Forces the port in 1 Gbps full duplex .
  - *SFP_Auto_AMS*: Automatically determines the speed of the SFP. There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to the missing standardized way of doing SFP auto detect some SFPs might not be detectable. The port is set in AMS mode. Cu port is set in *Auto* mode.
  - *100-FX*: SFP port is in 100-FX speed. Cu port is disabled.
  - *1000-X*: SFP port is in 1000-X speed. Cu port is disabled. Ports in AMS mode with 1000-X speed has Cu port preferred. Ports in AMS mode with 1000-X speed has fiber port preferred. Ports in AMS mode with 100-FX speed has fiber port preferred.

- **Advertise Duplex**: When duplex is set as auto that is, Autonegotiation, the port will only advertise the specified duplex as either Fdx or Hdx to the link partner. By default port will advertise all the supported duplexes if the Duplex is Auto.
- **Advertise Speed**: When Speed is set as auto that is, Autonegotiation, the port will only advertise the specified speeds (Speed10 Speed100 Speed1000) to the link partner. By default port will advertise all the supported speeds if speed is set as Auto.
- **Flow Control**: When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation.

  Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
- **Maximum Frame Size**: Enter the maximum frame size allowed for the switch port, including FCS. The range is 1518-10240 bytes.
- **Excessive Collision Mode**: Configure port transmit collision behavior. **Discard**: Discard frame after 16 collisions(default).

Related Topics

Monitoring Ports, on page 181



CHAPTER 7

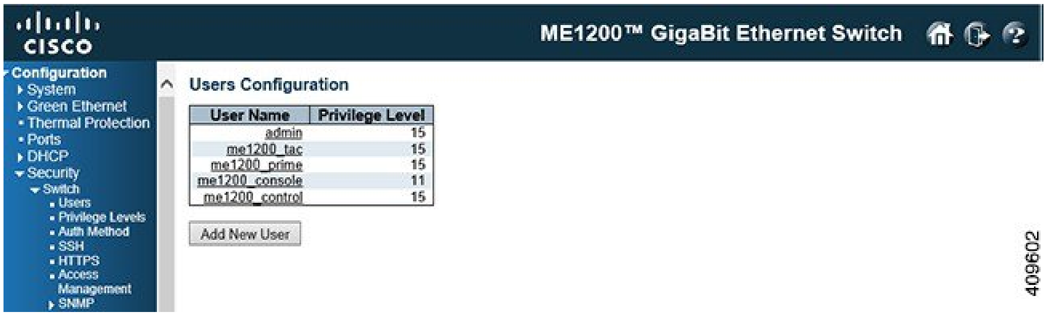
Configuring Security

The Security feature available on the ME 1200 Web GUI allows you to set the security configurations for the ME 1200.

Switch

Users Configuration

This option provides an overview of the current users. Currently, the only way to log in as another user on the web server is to close and reopen the browser.



Users Configuration

User Name	Privilege Level
admin	15
me1200_tac	15
me1200_prime	15
me1200_console	11
me1200_control	15

The displayed values for each user are:

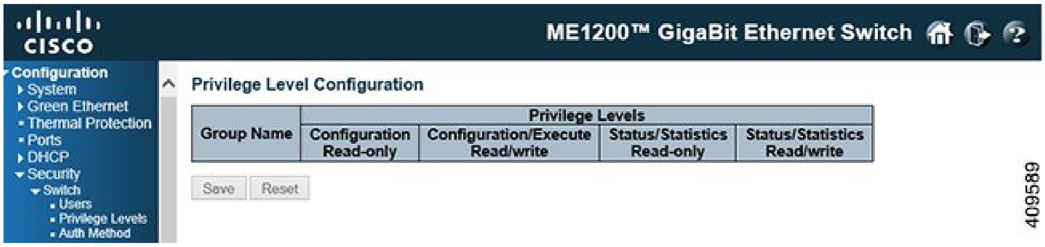
- **User Name**: The name identifying the user. This is also a link to edit a user.
- **Privilege Level**: The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, that is, that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software

upload, factory defaults, and so on) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

- **Add New User**: Click this button to add a new user.

Privilege Levels Configuration

This option provides an overview of the privilege levels configuration.



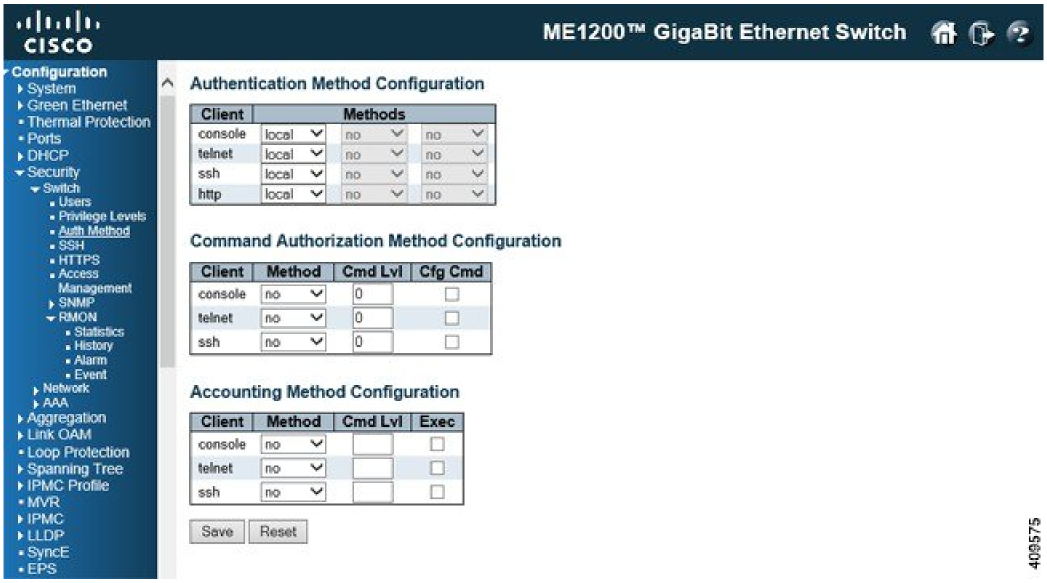
Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write

- **Group Name**: The name identifying the privilege group. In most cases, a privilege level group consists of a single module (for example, LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details:
    - *System*: Contact, Name, Location, Timezone, Daylight Saving Time, Log.
    - *Security*: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.
    - *IP*: Everything except **ping**.
    - *Port*: Everything except **VeriPHY**.
    - *Diagnostics*: 'ping' and **VeriPHY**.
    - *Maintenance*: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.
    - *Debug*: Only present in CLI.
- **Privilege Levels**: Every group has an authorization Privilege level for the following sub groups: *configuration read-only*, *configuration/execute read-write*, *status/statistics read-only*, *status/statistics read-write* (for example, for clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

Authentication Method Configuration

This option allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.



Authentication Method Configuration

Client	Methods		
console	local	no	no
telnet	local	no	no
ssh	local	no	no
http	local	no	no

Command Authorization Method Configuration

Client	Method	Cmd Lvl	Cfg Cmd
console	no	0	□
telnet	no	0	□
ssh	no	0	□

Accounting Method Configuration

Client	Method	Cmd Lvl	Exec
console	no		□
telnet	no		□
ssh	no		□

Save Reset

The table has one row for each client type and a number of columns which are as follows:

- **Client**: The management client for which the configuration below applies.
- **Methods**: Method can be set to one of the following values:
  - ◦ *no*: Authentication is disabled and login is not possible.
  - ◦ *local*: Uses the local user database on the switch for authentication.
  - ◦ *radius*: Uses one or more of the remote RADIUS servers for authentication.
  - ◦ *tacacs*: Uses one or more of the remote TACACS+ servers for authentication.

  Methods that involves remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as **local**. This will enable the management client to log in via the local user database if none of the configured authentication servers are alive.

Command Authorization Method Configuration

The command authorization section allows you to limit the CLI commands available to a user. The table has one row for each client type and a number of columns which are as follows:

- **Client**: The management client for which the configuration below applies.
- **Method**: This can be set to one of the following values:
  - *no*: Command authorization is disabled. User is granted access to CLI commands according to his privilege level.
  - *tacacs*: Uses one or more of the remote TACACS+ servers for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.

- **Cmd Lvl**: Authorizes all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15.
- **Cfg Cmd**: Also, authorizes configuration commands.

Accounting Method Configuration

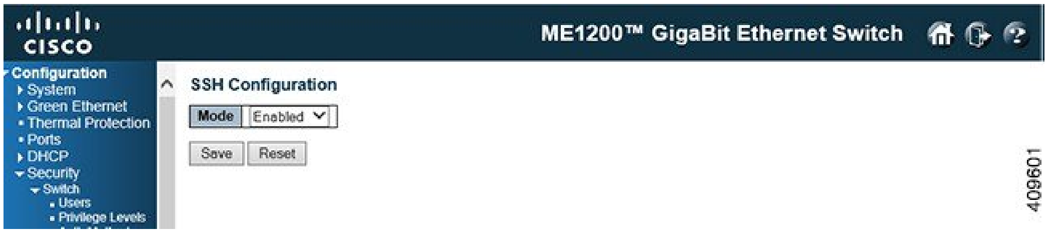
The accounting section allows you to configure command and exec (login) accounting. The table has one row for each client type and a number of columns which are as follows:

- **Client**: The management client for which the configuration below applies.
- **Method**: can be set to one of the following values:
    - ◦ *no*: Accounting is disabled.
    - ◦ *tacacs*: Uses one or more of the remote TACACS+ servers for accounting.

- **Cmd Lvl**: Enables accounting of all commands with a privilege level higher than or equal to this level.Valid values are in the range 0 to 15. Leave the field empty to disable command accounting.
- **Exec**: Enables exec (login) accounting.

SSH Configuration

This option allows you to configure SSH.



SSH Configuration

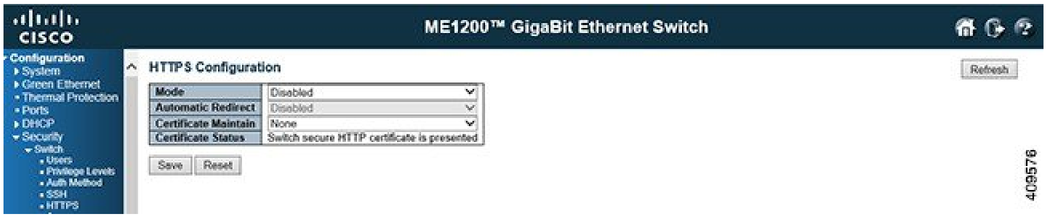
Mode: Enabled

The **Mode** option indicates the SSH mode operation. Possible modes are:

- *Enabled*: Enables SSH mode operation.
- *Disabled*: Disables SSH mode operation.

HTTPS Configuration

This option allows you to configure HTTPS.



HTTPS Configuration

Mode	Disabled
Automatic Redirect	Disabled
Certificate Maintain	None
Certificate Status	Switch secure HTTP certificate is presented

- **Mode**: Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. Possible modes are:
  - ◦ *Enabled*: Enables HTTPS mode operation.
  - ◦ *Disabled*: Disables HTTPS mode operation.

- **Automatic Redirect**: Indicates the HTTPS redirect mode operation. It is only significant if HTTPS mode *Enabled* is selected. Automatically redirects web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled.

  The browser may not allow the redirect operation due to the security consideration unless the switch certificate is trusted to the browser. Initialize the HTTPS connection manually under this case. Possible modes are:
  - *Enabled*: Enables HTTPS redirect mode operation.
  - *Disabled*: Disables HTTPS redirect mode operation.

- **Certificate Maintain**: This field only can be configured when HTTPS is disabled. It is used to maintain the certification. Possible actions are:
  - ◦ *None*: No action for certification.
  - ◦ *Delete*: To delete certification.
  - ◦ *Upload*: To upload certification, there are two types of upload methods that can be selected: Web Browser or URL.
  - ◦ *Generate*: To generate certification.

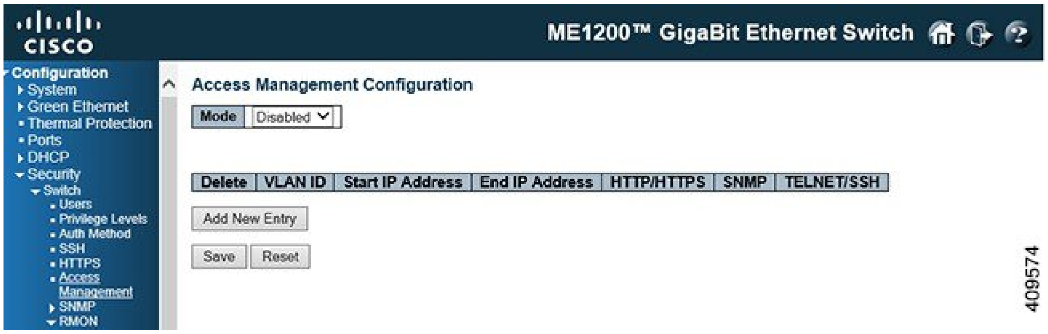
- **Certificate Algorithm**: HTTPS can generate two types of certification. Possible types are:
  - ◦ *RSA*: RSA certification.
  - ◦ *DSA*: DSA certification.

- **PassPhrase**: The pattern is used for encrypting the certification.
- **Certificate Upload**: Possible modes are:
  - ◦ *Web Browser*: To Upload certification via Web browser.
  - ◦ *URL*: To Upload certification via URL, the supported protocols are HTTP, TFTP and FTP, the URL format is **<protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]**

- **Certificate Status**: Possible status is:
    - *Switch secure HTTP certificate is presented*: The certification is stored in HTTPS' database.
    - *Switch secure HTTP certificate is not presented*: No certification is stored in HTTPS' database.
    - *Switch secure HTTP certificate is generating*: The certification is generating.

Access Management Configuration

This option allows you to configure access management. The maximum number of entries is 16. If the type of the application matches any one of the access management entries, it allows access to the switch.



Access Management Configuration

Mode: Disabled

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH

- **Mode**: Indicates the access management mode operation. Possible modes are:
    - *Enabled*: Enables access management mode operation.
    - *Disabled*: Disables access management mode operation.

- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **VLAN ID**: Indicates the VLAN ID for the access management entry.
- **Start IP address**: Indicates the start IP address for the access management entry.
- **End IP address**: Indicates the end IP address for the access management entry.
- **HTTP/HTTPS**: Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.
- **SNMP**: Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.
- **TELNET/SSH**: Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.
- **Add New Entry**: Click this button to add a new access management entry.

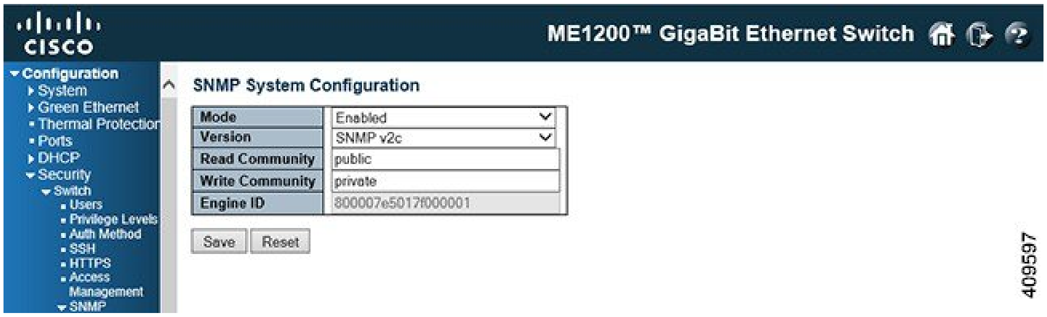
Related Topics

Monitoring Security, on page 193

SNMP

SNMP System Configuration

This option allows you to system configure the SNMP feature.



SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

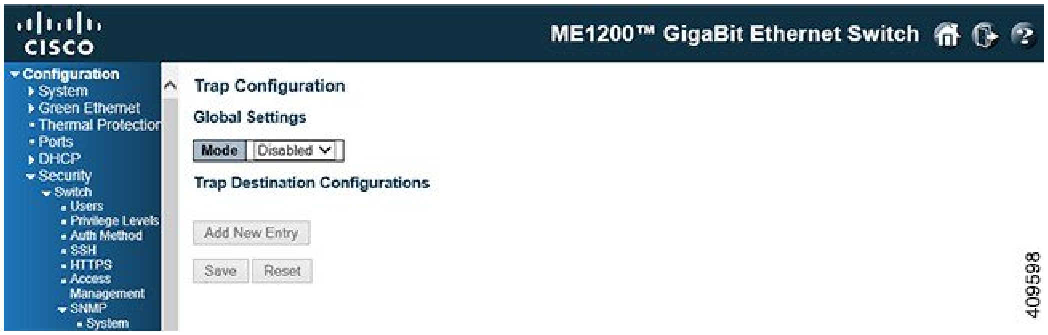
- **Mode**: Indicates the SNMP mode operation. Possible modes are:
  - *Enabled*: Enables SNMP mode operation.
  - *Disabled*: Disables SNMP mode operation.

- **Version**: Indicates the SNMP supported version. Possible versions are:
  - *SNMP v1*: Sets SNMP supported version 1.
  - *SNMP v2c*: Sets SNMP supported version 2c.
  - *SNMP v3*: Sets SNMP supported version 3.

- **Read Community**: Indicates the community read access string to permit access to SNMP agent. The allowed string length is 1 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string is associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.
- **Write Community**: Indicates the community write access string to permit access to SNMP agent. The allowed string length is 1 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string is associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.
- **Engine ID**: Indicates the SNMPv3 engine ID. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

SNMP Trap Configuration

This option allows you to configure the SNMP trap feature.



Trap Configuration

Global Settings

Mode: Disabled

Trap Destination Configurations

Global Settings

- **Mode**: Indicates the trap mode operation. Possible modes are as follows:
    - *Enabled*: Enables SNMP trap mode operation.
    - *Disabled*: Disables SNMP trap mode operation.

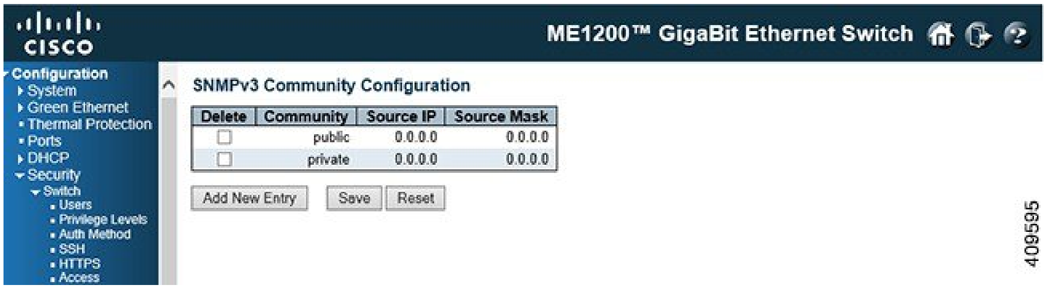
Trap Destination Configurations

Configure trap destinations on this page.

- **Name**: Indicates the name of the trap configuration.
- **Enable**: Indicates the trap destination mode operation. Possible modes are as follows:
    - *Enabled*: Enables SNMP trap mode operation.
    - *Disabled*: Disables SNMP trap mode operation.
- **Version**: Indicates the SNMP trap supported version. Possible versions are as follows:
    - *SNMPv1*: Sets SNMP trap supported version 1.
    - *SNMPv2c*: Sets SNMP trap supported version 2c. SNMPv3: Set SNMP trap supported version 3.
- **Destination Address**: Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w') as well as a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash. Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
- **Destination port**: Indicates the SNMP trap destination port. SNMP Agent sends an SNMP message via this port. The port range is 1~65535.

SNMPv3 Community Configuration

This option allows you to configure SNMPv3 community table. The entry index key is Community.



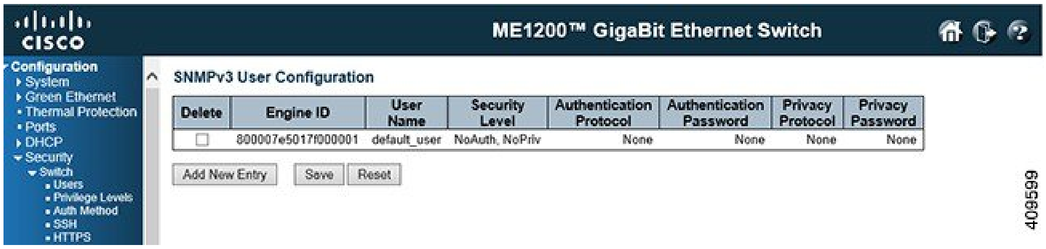
SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask
□	public	0.0.0.0	0.0.0.0
□	private	0.0.0.0	0.0.0.0

- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **Community**: Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.
- **Source IP**: Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.
- **Source Mask**: Indicates the SNMP access source address mask.
- **Add New Entry**: Click this button to add a new community entry.

SNMPv3 User Configuration

This option allows you to configure SNMPv3 user table. The entry index keys are Engine ID and User Name.



SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
□	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **Engine ID**: An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID

of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is a local user; otherwise it is a remote user.

- **User Name**: A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
- **Security Level**: Indicates the security model that this entry should belong to. Possible security models are:
    - *NoAuth, NoPriv*: No authentication and no privacy.
    - *Auth, NoPriv*: Authentication and no privacy.
    - *Auth, Priv*: Authentication and privacy.

    The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.

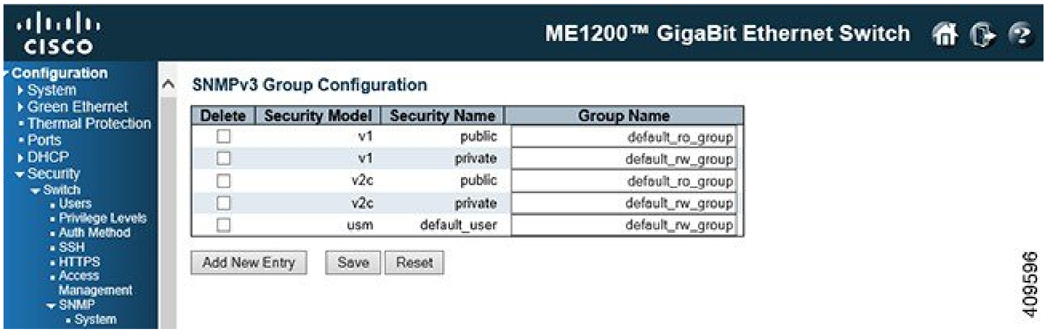
- **Authentication Protocol**: Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:
    - *None*: No authentication protocol.
    - *MD5*: An optional flag to indicate that this user uses MD5 authentication protocol.
    - *SHA*: An optional flag to indicate that this user uses SHA authentication protocol.

    The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.

- **Authentication Password**: A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.
- **Privacy Protocol**: Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:
    - *None*: No privacy protocol.
    - *DES*: An optional flag to indicate that this user uses DES authentication protocol.
    - *AES*: An optional flag to indicate that this user uses AES authentication protocol.
- **Privacy Password**: A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.
- **Add New Entry**: Click this button to add a new user entry.

SNMPv3 Group Configuration

This option allows you to configure the SNMPv3 group table. The entry index keys are Security Model and Security Name.



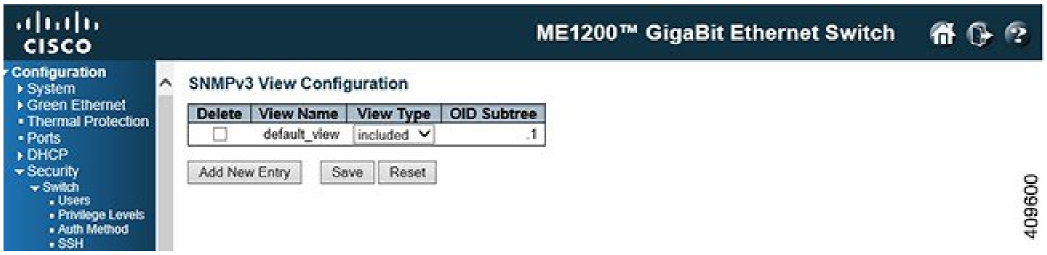
SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
□	v1	public	default_ro_group
□	v1	private	default_rw_group
□	v2c	public	default_ro_group
□	v2c	private	default_rw_group
□	usm	default_user	default_rw_group

- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **Security Model**: Indicates the security model that this entry should belong to. Possible security models are as follows:
  - *v1*: Reserved for SNMPv1.
  - *v2c*: Reserved for SNMPv2c.
  - *usm*: User-based Security Model (USM).
- **Security Name**: A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
- **Group Name**: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
- **Add New Entry**: Click this button to add a new group entry.

SNMPv3 View Configuration

This option allows you to configure the SNMPv3 view table. The entry index keys are View Name and OID Subtree.



SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
□	default_view	included	.1

- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **View Name**: A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
- **View Type**: Indicates the view type that this entry should belong to. Possible view types are:

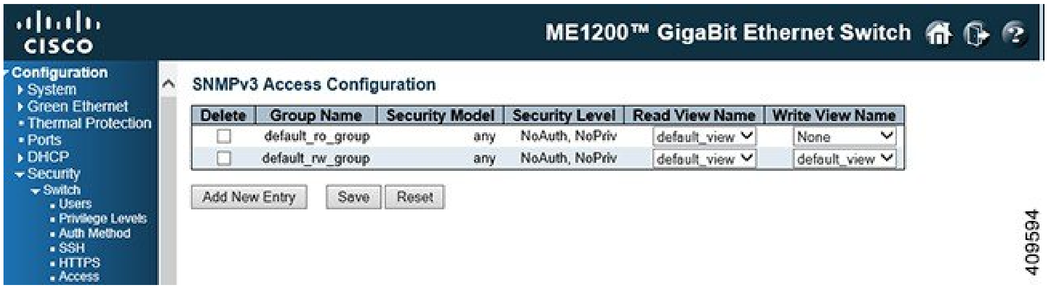
- ◦ *included*: An optional flag to indicate that this view subtree should be included.
- ◦ *excluded*: An optional flag to indicate that this view subtree should be excluded.

  In general, if the view type of a view entry is *excluded*, there should be another view entry existing with view type as *included* and its OID subtree should overstep the *excluded* view entry.

- **OID Subtree**: The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).
- **Add New Entry**: Click this button to add a new view entry.

SNMPv3 Access Configuration

This option allows you to configure the SNMPv3 access table. The entry index keys are Group Name, Security Model and Security Level.



SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	default_ro_group	any	NoAuth, NoPriv	default_view	None
□	default_rw_group	any	NoAuth, NoPriv	default_view	default_view

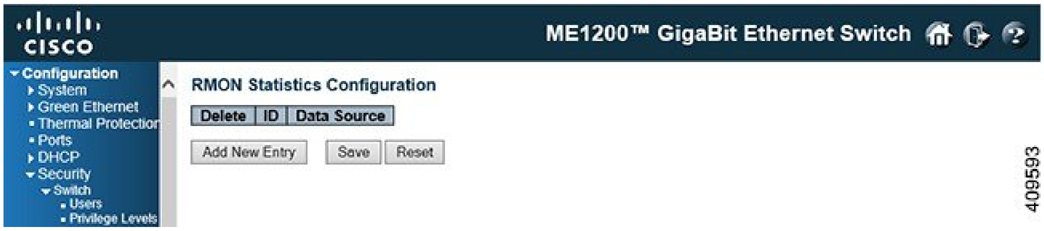
- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **Group Name**: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
- **Security Model**: Indicates the security model that this entry should belong to. Possible security models are as follows:
  - ◦ *any*: Any security model accepted(v1|v2c|usm).
  - ◦ *v1*: Reserved for SNMPv1.
  - ◦ *v2c*: Reserved for SNMPv2c.
  - ◦ *usm*: User-based Security Model (USM).
- **Security Level**: Indicates the security model that this entry should belong to. Possible security models are as follows:
  - ◦ *NoAuth, NoPriv*: No authentication and no privacy.
  - ◦ *Auth, NoPriv*: Authentication and no privacy.
  - ◦ *Auth, Priv*: Authentication and privacy.

- **Read View Name**: The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
- **Write View Name**: The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
- **Add New Entry**: Click this button to add a new access entry.

RMON

RMON Statistics Configuration

This option allows you to configure the RMON Statistics table. The entry index key is ID.



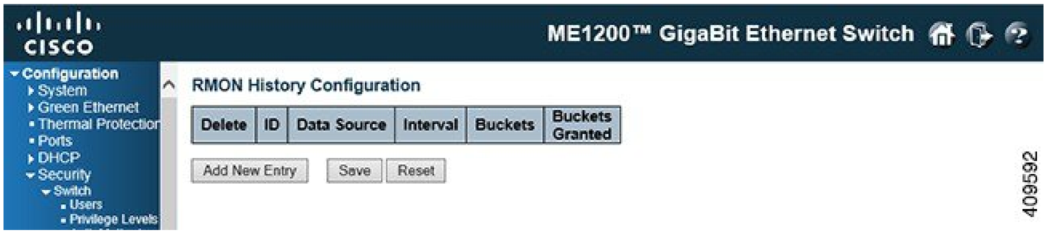
- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **ID**: Indicates the index of the entry. The range is from 1 to 65535.
- **Data Source**: Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.
- **Add New Entry**: Click this button to add a new community entry.

Related Topics

Monitoring Security, on page 193

RMON History Configuration

This option allows you to configure the RMON History table. The entry index key is ID.



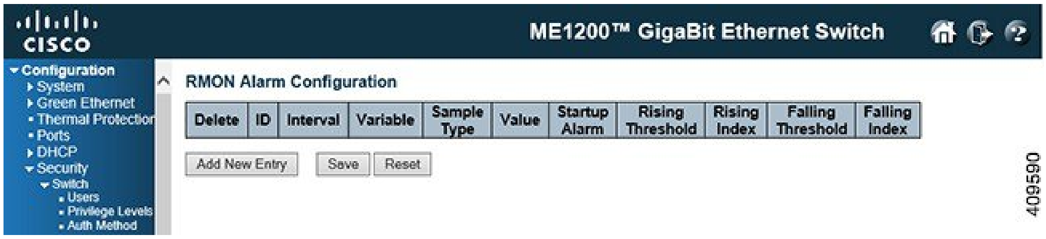
- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **ID**: Indicates the index of the entry. The range is from 1 to 65535.
- **Data Source**: Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.
- **Interval**: Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
- **Buckets**: Indicates the maximum data entries associated with this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.
- **Buckets Granted**: The number of data entries saved in the RMON.
- **Add New Entry**: Click this button to add a new community entry.

Related Topics

Monitoring Security, on page 193

RMON Alarm Configuration

This option allows you to configure the RMON Alarm table. The entry index key is ID.



RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index

- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **ID**: Indicates the index of the entry. The range is from 1 to 65535.
- **Interval**: Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.
- **Variable**: Indicates the particular variable to be sampled, the possible variables are as follows:
    - *InOctets*: The total number of octets received on the interface, including framing characters.
    - *InUcastPkts*: The number of uni-cast packets delivered to a higher-layer protocol.
    - *InNUcastPkts*: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.
    - *InDiscards*: The number of inbound packets that are discarded even the packets are normal.
    - *InErrors*: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

    - *InUnknownProtos*: The number of the inbound packets that were discarded because of the unknown or un-support protocol.
    - *OutOctets*: The number of octets transmitted out of the interface , including framing characters.
    - *OutUcastPkts*: The number of uni-cast packets that request to transmit.
    - *OutNUcastPkts*: The number of broad-cast and multi-cast packets that request to transmit.
    - *OutDiscards*: The number of outbound packets that are discarded event the packets is normal.
    - *OutErrors*: The number of outbound packets that could not be transmitted because of errors.
    - *OutQLen*: The length of the output packet queue (in packets).

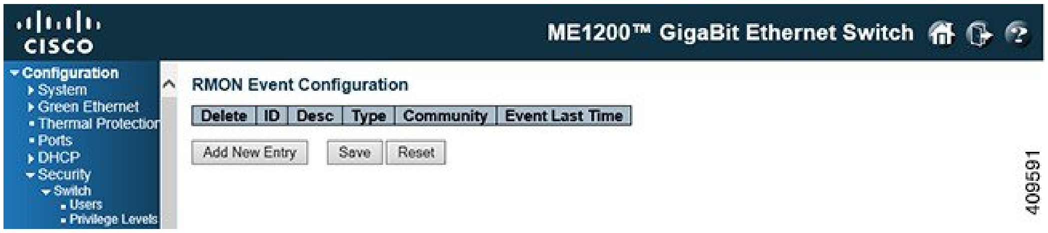
- **Sample Type**: The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are as follows:
    - *Absolute*: Get the sample directly.
    - *Delta*: Calculate the difference between samples (default).
- **Value**: The value of the statistic during the last sampling period.
- **Startup Alarm**: The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are as follows:
    - *Rising* Trigger alarm when the first value is larger than the rising threshold.
    - *Falling* Trigger alarm when the first value is less than the falling threshold.
    - *RisingOrFalling* Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).
- **Rising Threshold**: Rising threshold value (-2147483648-2147483647).
- **Rising Index**: Rising event index (1-65535).
- **Falling Threshold**: Falling threshold value (-2147483648-2147483647).
- **Falling Index**: Falling event index (1-65535).
- **Add New Entry**: Click this button to add a new community entry.

Related Topics

Monitoring Security, on page 193

RMON Event Configuration

This option allows you to configure the RMON Event table. The entry index key is ID.



- **Delete**: Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
- **ID**: Indicates the index of the entry. The range is from 1 to 65535.
- **Desc**: Indicates this event, the string length is from 0 to 127, default is a null string.
- **Type**: Indicates the notification of the event, the possible types are as follows:
    - *none*: No SNMP log is created, no SNMP trap is sent
    - *log*: Create SNMP log entry when the event is triggered.
    - *snmptrap*: Send SNMP trap when the event is triggered.
    - *logandtrap*: Create SNMP log entry and sent SNMP trap when the event is triggered.
- **Community**: Specify the community when trap is sent, the string length is from 0 to 127, default is *public*.
- **Event Last Time**: Indicates the value of sysUpTime at the time this event entry last generated an event.
- **Add New Entry**: Click this button to add a new community entry.

Related Topics

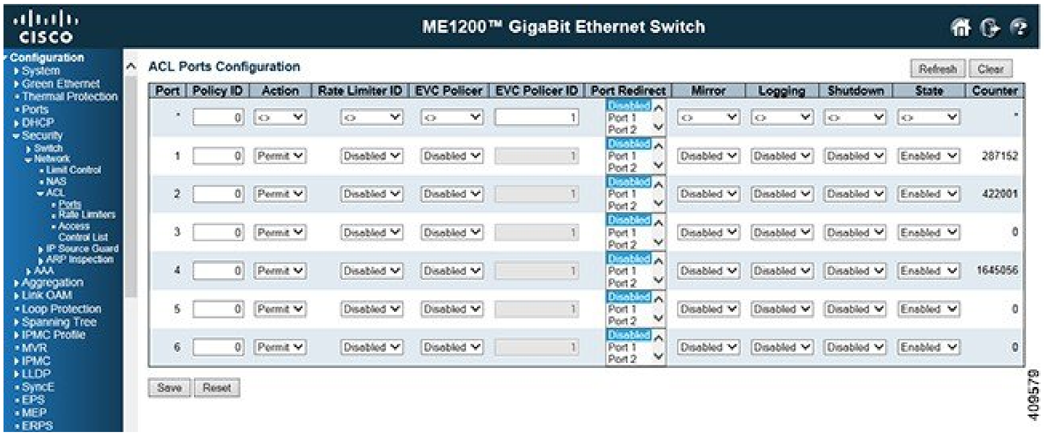
Monitoring Security, on page 193

Network

ACL

ACL Ports Configuration

This option allows you to configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.



ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	EVC Policer	EVC Policer ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	<>	1	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	287152
2	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	422001
3	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	1645056
5	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

- **Port**: The logical port for the settings contained in the same row.
- **Policy ID**: Select the policy to apply to this port. The allowed values are 0 through 63. The default value is 0.
- **Action**: Select whether forwarding is permitted *Permit* or denied *Deny*. The default value is *Permit*.
- **Rate Limiter ID**: Select which rate limiter to apply on this port. The allowed values are *Disabled* or the values 1 through 16. The default value is *Disabled*.
- **EVC Policer**: Select whether EVC policer is enabled or disabled. The default value is *Disabled*. Note that ACL rate limiter and EVC policer can not both be enabled.
- **EVC Policer ID**: Select which EVC policer ID to apply on this port. The allowed values are Disabled or the values 1 through 1022.
- **Port Redirect**: Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it cannot be set when action is permitted. The default value is *Disabled*.
- **Mirror**: Specifies the mirror operation of this port. The allowed values are:
    - *Enabled*: Frames received on the port are mirrored.
    - *Disabled*: Frames received on the port are not mirrored. The default value is *Disabled*.
- **Logging**: Specifies the logging operation of this port. Notice that the logging message does not include the 4 bytes CRC. The allowed values are:
    - *Enabled*: Frames received on the port are stored in the System Log.
    - *Disabled*: Frames received on the port are not logged. The default value is *Disabled*.

Note The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.

- **Shutdown**: Specifies the port shut down operation of this port. The allowed values are:
    - *Enabled*: If a frame is received on the port, the port will be disabled.
    - *Disabled*: Port shut down is disabled. The default value is *Disabled*.

Note The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).

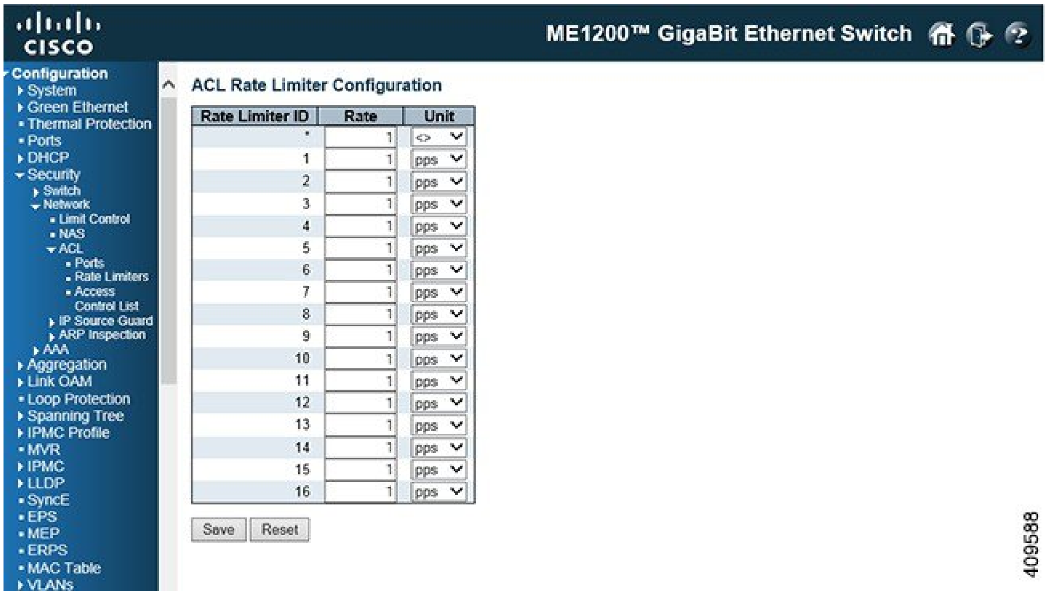
- **State**: Specifies the port state of this port. The allowed values are:
    - *Enabled*: To reopen ports by changing the volatile port configuration of the ACL user module.
    - *Disabled*: To close ports by changing the volatile port configuration of the ACL user module. The default value is *Enabled*.
- **Counter**: Counts the number of frames that match this ACE.

Related Topics

Monitoring Security, on page 193

ACL Rate Limiter Configuration

This option allows you to configure the rate limiter for the ACL of the switch.



ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	1	<>
1	1	pps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

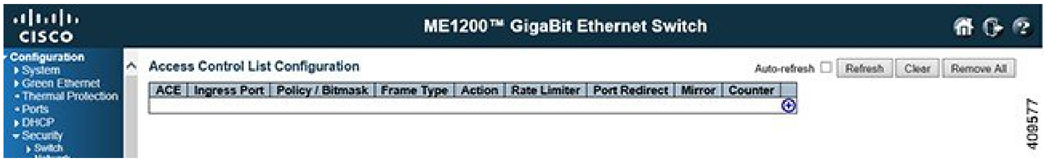
- **Rate Limiter ID**: The rate limiter ID for the settings contained in the same row and its range is 1 to 16.
- **Rate**: The rate range is located 0-128k in pps. The valid rate is 0 - 99, 100, 100, 100, ..., 3276700 in pps or 0, 100, 100, 100, ..., 1000000 in kbps.
- **Unit**: Specify the rate unit. The allowed values are as follows:
    - *pps*: packets per second.
    - *kbps*: Kbit per second.

Related Topics

Monitoring Security, on page 193

Access Control List Configuration

This option shows the Access Control List (ACL) that is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 512 on each switch.



Access Control List Configuration

Auto-refresh □ Refresh Clear Remove All

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter

ClickAdd **ACE to end of list** icon to add a new ACE to the list. The reserved ACEs used for internal protocol cannot be edited or deleted, the order sequence cannot be changed, and the priority is highest.

- **ACE**: Indicates the ACE ID.
- **Ingress Port**: Indicates the ingress port of the ACE. Possible values are:
  - *All*: The ACE will match all ingress port.
  - *Port*: The ACE will match a specific ingress port.
- **Policy / Bitmask**: Indicates the policy number and bitmask of the ACE.
- *Frame Type*: Indicates the frame type of the ACE. Possible values are:
  - *Any*: The ACE will match any frame type.
  - *EType*: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.
  - *ARP*: The ACE will match ARP/RARP frames.
  - *IPv4*: The ACE will match all IPv4 frames.
  - *IPv4/ICMP*: The ACE will match IPv4 frames with ICMP protocol.
  - *IPv4/UDP*: The ACE will match IPv4 frames with UDP protocol.
  - *IPv4/TCP*: The ACE will match IPv4 frames with TCP protocol.
  - *IPv4/Other*: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
  - *IPv6*: The ACE will match all IPv6 standard frames.
- **Action**: Indicates the forwarding action of the ACE.
  - **Permit**: Frames matching the ACE may be forwarded and learned.
  - **Deny**: Frames matching the ACE are dropped.
  - **Filter**: Frames matching the ACE are filtered.

- **Rate Limiter**: Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When *Disabled* is displayed, the rate limiter operation is disabled.
- **Port Redirect**: Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are *Disabled* or a specific port number. When Disabled is displayed, the port redirect operation is disabled.
- **Mirror**: Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:
    - *Enabled*: Frames received on the port are mirrored.
    - *Disabled*: Frames received on the port are not mirrored. The default value is *Disabled*.
- **Counter**: The counter indicates the number of times the ACE was hit by a frame.
- Modification icons: You can modify each Access Control Entry (ACE) in the table by using the following icons:
    - **Insert new ACE before this ACE** icon: Inserts a new ACE before the current row.
    - **Edit ACE** icon: Edits the ACE row.
    - **Move ACE up** icon: Moves the ACE up the list.
    - **Move ACE down** icon: Moves the ACE down the list.
    - **Delete ACE** icon: Deletes the ACE.
    - **Add ACE to end of list** icon: The lowest plus sign adds a new entry at the bottom of the ACE listings.

Related Topics

Monitoring Security, on page 193

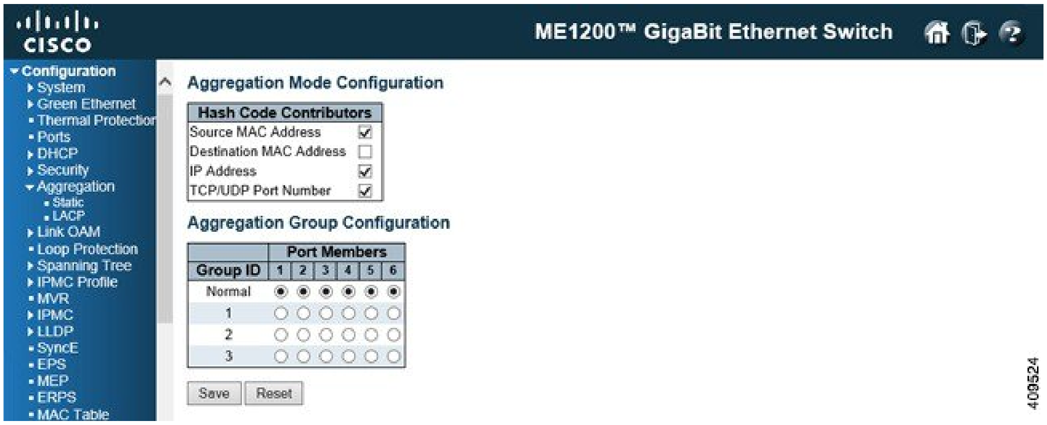
CHAPTER 8

Configuring Aggregation

The Aggregation feature available on ME1200 Web GUI allows you to set configurations for static aggregation mode/group and dynamic aggregation using LACP.

Aggregation Configuration

This option allows you to configure the Aggregation hash mode and the aggregation group.



Aggregation Mode Configuration

Hash Code Contributors	
Source MAC Address	☑
Destination MAC Address	□
IP Address	☑
TCP/UDP Port Number	☑

Aggregation Group Configuration

	Port Members					
Group ID	1	2	3	4	5	6
Normal	●	●	●	●	●	●
1	○	○	○	○	○	○
2	○	○	○	○	○	○
3	○	○	○	○	○	○

Hash Code Contributors

- **Source MAC Address**: The Source MAC Address can be used to calculate the destination port for the frame. You can check or uncheck the **Source MAC Address** check box to enable or disable this option. By default, **Source MAC Address** is enabled.
- **Destination MAC Address**: The Destination MAC Address can be used to calculate the destination port for the frame. You can check or uncheck the **Destination MAC Address** check box to enable or disable this option. By default, **Destination MAC Address** is disabled.

- **IP Address**: The IP address can be used to calculate the destination port for the frame. You can check or uncheck the **IP Address** check box to enable or disable this option. By default, **IP Address** is enabled.
- **TCP/UDP Port Number**: The TCP/UDP port number can be used to calculate the destination port for the frame. You can check or uncheck the **TCP/UDP Port Number** check box to enable or disable his option. By default, **TCP/UDP Port Number** is enabled.

Aggregation Group Configuration

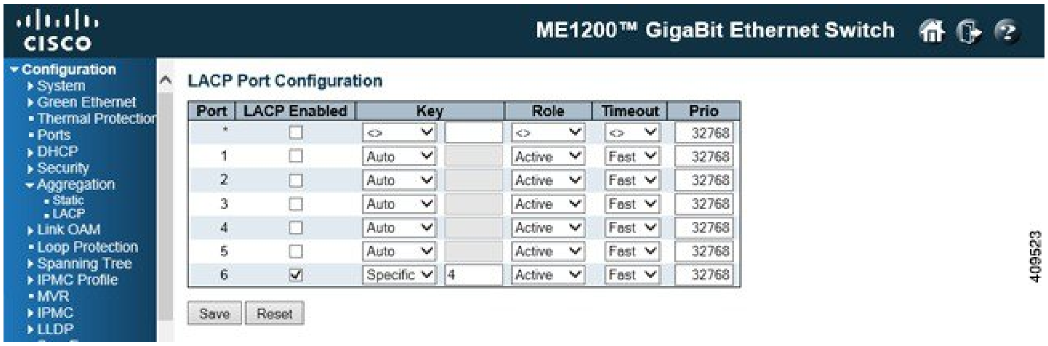
- **Group ID**: Indicates the group ID for the settings contained in the same row. Group ID **Normal** indicates there is no aggregation. Only one group ID is valid per port.
- **Port Members**: Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no port belongs to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

Related Topics

Monitoring Aggregation, on page 201

LACP Configuration

This option allows you to inspect the current LACP port configurations and change them.



LACP Port Configuration

Port	LACP Enabled	Key		Role	Timeout	Prio
*	□	<>		<>	<>	32768
1	□	Auto		Active	Fast	32768
2	□	Auto		Active	Fast	32768
3	□	Auto		Active	Fast	32768
4	□	Auto		Active	Fast	32768
5	□	Auto		Active	Fast	32768
6	☑	Specific	4	Active	Fast	32768

- **Port**: The switch port number.
- **LACP Enabled**: Controls whether LACP is enabled on this switch port. LACP forms an aggregation when two or more ports are connected to the same partner.
- **Key**: The Key value incurred by the port, range 1-65535. The ***Auto*** setting sets the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
- **Role**: The Role shows the LACP activity status. The ***Active*** setting transmits LACP packets each second, while ***Passive*** setting waits for a LACP packet from a partner.
- **Timeout**: The Timeout controls the period between BPDU transmissions. The ***Fast*** setting transmits LACP packets each second, while ***Slow*** setting waits for 30 seconds before sending a LACP packet.

- **Prio**: The Prio controls the priority of the port, range 1-65535. If the LACP partner wants to form a larger group than is supported by this device then this parameter controls the ports that are active and the ports that are in a backup role. Lower number means a higher priority.

Related Topics

Monitoring Aggregation, on page 201

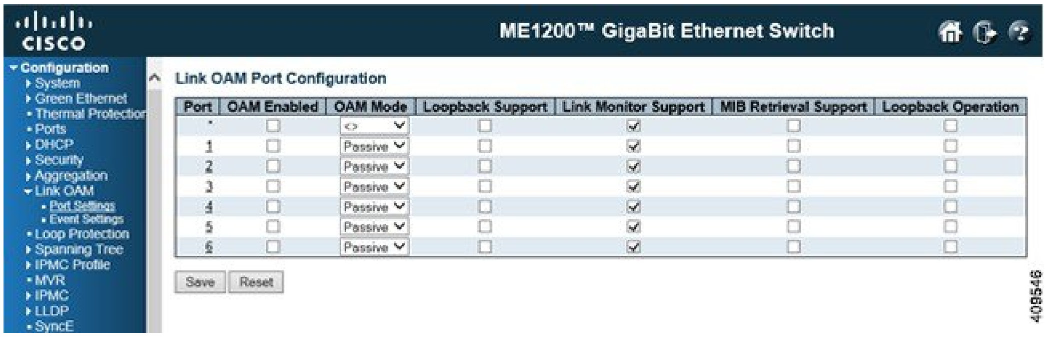
CHAPTER 9

Configuring Link OAM

The Link OAM feature available on the ME 1200 Web GUI allows you to configure the Link OAM port and the Link Event for a given port.

Link OAM Port Configuration

This option allows you to inspect the current Link OAM port configurations and change them as well.



Link OAM Port Configuration

Port	OAM Enabled	OAM Mode	Loopback Support	Link Monitor Support	MIB Retrieval Support	Loopback Operation
*	□	<>	□	☑	□	□
1	□	Passive	□	☑	□	□
2	□	Passive	□	☑	□	□
3	□	Passive	□	☑	□	□
4	□	Passive	□	☑	□	□
5	□	Passive	□	☑	□	□
6	□	Passive	□	☑	□	□

- **Port**: The switch port number.
- **OAM Enabled**: Controls whether Link OAM is enabled on this switch port. Enabling Link OAM provides the network operators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions.
- **OAM Mode**: Configures the OAM Mode as Active or Passive. The default mode is Passive.
    - *Active*: DTE is configured in Active mode initiate the exchange of Information OAMPDUs as defined by the Discovery process. Once the Discovery process completes, Active DTEs are permitted to send any OAMPDU while connected to a remote OAM peer entity in Active mode. Active DTEs operate in a limited respect if the remote OAM entity is operating in Passive mode. Active devices

should not respond to OAM remote loopback commands and variable requests from a Passive peer.

◦ *Passive*: DTE is configured in Passive mode do not initiate the Discovery process. Passive DTE's react to the initiation of the Discovery process by the remote DTE. This eliminates the possibility of passive to passive links. Passive DTE's shall not send Variable Request or Loopback Control OAMPDUs.

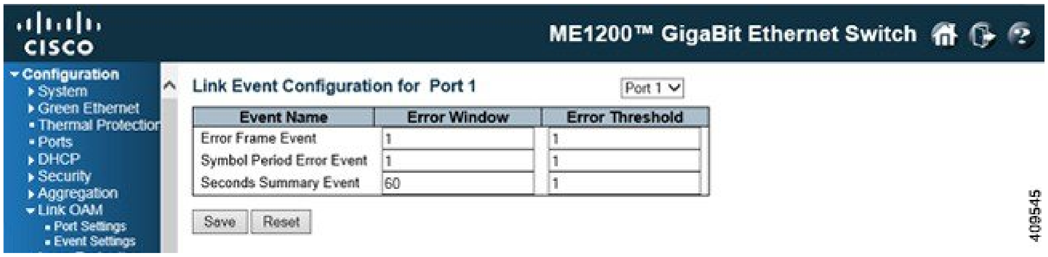
- **Loopback Support**: Controls whether the loopback support is enabled for the switch port. Link OAM remote loopback can be used for fault localization and link performance testing. Enabling the loopback support will allow the DTE to execute the remote loopback command that helps in the fault detection.
- **Link Monitor Support**: Controls whether the Link Monitor support is enabled for the switch port. On enabling the Link Monitor support, the DTE supports event notification that permits the inclusion of diagnostic information.
- **MIB Retrieval Support**: Controls whether the MIB Retrieval Support is enabled for the switch port. On enabling the MIB retrieval support, the DTE supports polling of various Link OAM based on the contents of the MIB variables.
- **Loopback Operation**: If the Loopback support is enabled, enabling this field will start a loopback operation for the port.

Related Topics

Monitoring Link OAM, on page 187

Link OAM Link Event Configuration

This option allows you to inspect the current Link OAM Link Event configurations and change them.



Link Event Configuration for Port 1

Event Name	Error Window	Error Threshold
Error Frame Event	1	1
Symbol Period Error Event	1	1
Seconds Summary Event	60	1

- **Port**: The switch port number.
- **Event Name**: Name of the Link Event which is being configured.
- **Error Window**: Represents the window period in the order of 1 sec for the observation of various link events.
- **Error Threshold**: Represents the threshold value for the window period for the appropriate Link event so as to notify the peer of this error.
- **Error Frame Event**: Counts the number of errored frames detected during the specified period. The period is specified by a time interval (Window in order of 1 sec). This event is generated if the errored frame count is equal to or greater than the specified threshold for that period (Period Threshold). Errored

frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Error Frame Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-4294967295 and its default value is '0'.

- **Symbol Period Error Event**: Counts the number of symbol errors that occurred during the specified period. The period is specified by the number of symbols that can be received in a time interval on the underlying physical layer. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period. Error Window for 'Symbol Period Error Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-4294967295 and its default value is '0'.
- **Seconds Summary Event**: The Errored Frame Seconds Summary Event TLV counts the number of errored frame seconds that occurred during the specified period. The period is specified by a time interval. This event is generated if the number of errored frame seconds is equal to or greater than the specified threshold for that period. An errored frame second is a one second interval wherein at least one frame error was detected. Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Seconds Summary Event' must be an integer value between 10-900 and its default value is '60'. Whereas Error Threshold must be between 0-65535 and its default value is '1'.

Note The port select box determines which port is affected by clicking the buttons.

Related Topics

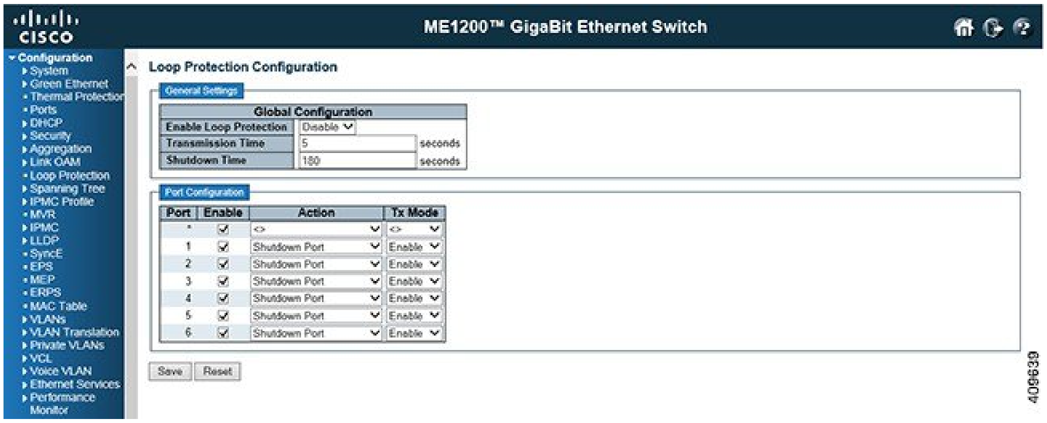
Monitoring Link OAM, on page 187

CHAPTER 10

Configuring Loop Protection

Loop Protection Configuration

This feature allows you to inspect the current Loop Protection configurations and change them.



Loop Protection Configuration

Global Configuration		
Enable Loop Protection	Disable	
Transmission Time	5	seconds
Shutdown Time	180	seconds

Port	Enable	Action	Tx Mode
*	☑	<>	<>
1	☑	Shutdown Port	Enable
2	☑	Shutdown Port	Enable
3	☑	Shutdown Port	Enable
4	☑	Shutdown Port	Enable
5	☑	Shutdown Port	Enable
6	☑	Shutdown Port	Enable

General Settings

- **Enable Loop Protection**: Controls whether loop protections is enabled (as a whole). Transmission Time. The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds. Default value is 5 seconds.
- **Shutdown Time**: The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart). Default value is 180 seconds.

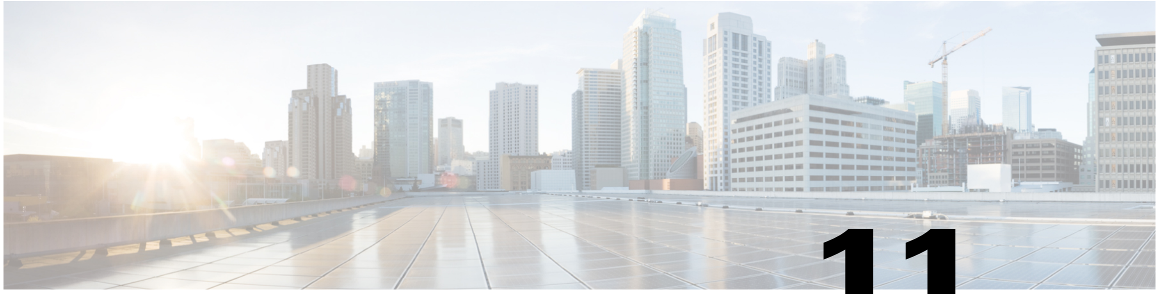
Port Configuration

- **Port**: The switch port number of the port.
- **Enable**: Controls whether loop protection is enabled on this switch port

- **Action**: Configures the action performed when a loop is detected on a port. Valid values are *Shutdown Port*, *Shutdown Port* and *Log* or *Log Only*.
- **Tx Mode**: Controls whether the port is actively generating loop protection PDUs, or whether it is just passively looking for looped PDUs.

Related Topics

Monitoring Loop Protection, on page 205



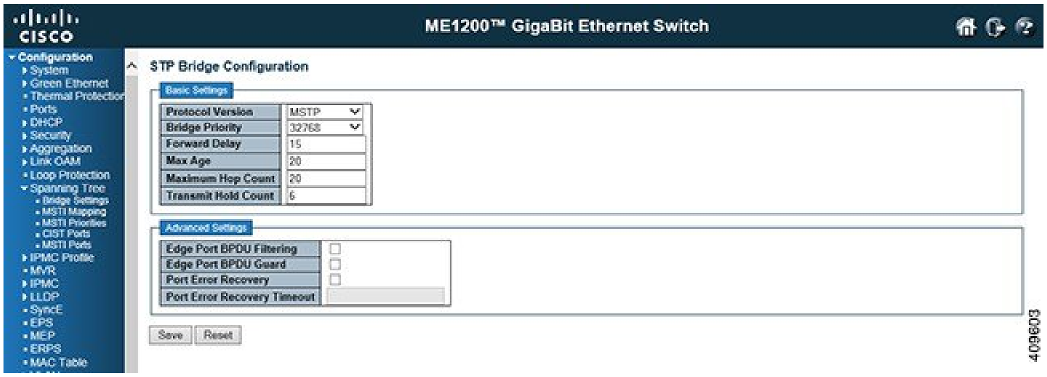
CHAPTER 11

Configuring Spanning Tree

The Spanning Tree feature available on the ME 1200 Web GUI allows you to configure the Bridge, MSTI, and CIST settings.

STP Bridge Configuration

This option allows you to configure STP system settings. The settings are used by all STP Bridge instances in the switch.



STP Bridge Configuration

Basic Settings

Protocol Version	MSTP
Bridge Priority	32768
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	□
Edge Port BPDU Guard	□
Port Error Recovery	□
Port Error Recovery Timeout	

Basic Settings

- **Protocol Version**: The MSTP/RSTP/STP protocol version setting. Valid values are STP, RSTP, and MSTP.

- **Bridge Priority**: Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

  For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
- **Forward Delay**: The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.
- **Max Age**: The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.
- **Maximum Hop Count**: This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.
- **Transmit Hold Count**: The number of BPDUs a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDUs per second.

Advanced Settings

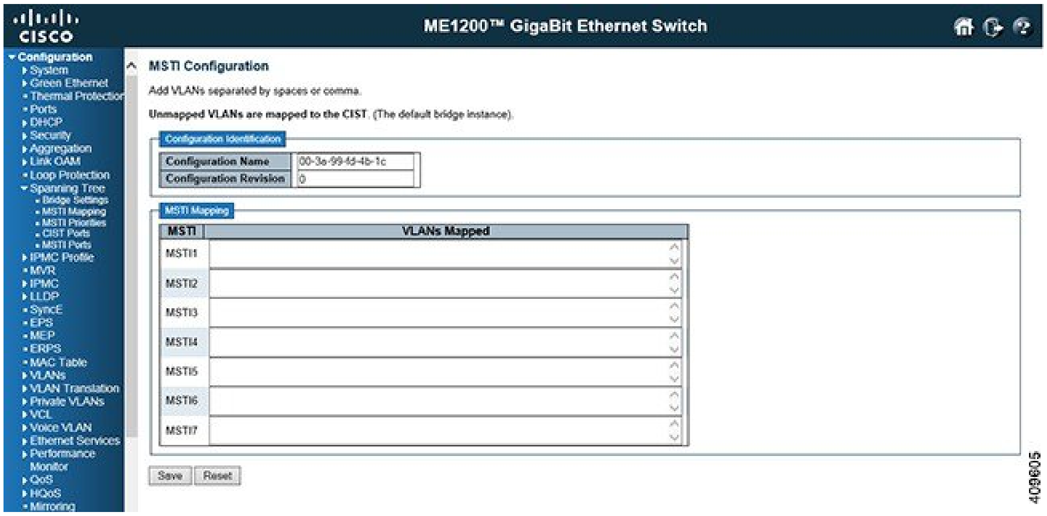
- **Edge Port BPDU Filtering**: Control whether a port explicitly configured as Edge will transmit and receive BPDUs.
- **Edge Port BPDU Guard**: Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state and will be removed from the active topology.
- **Port Error Recovery**: Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.
- **Port Error Recovery Timeout**: The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

Related Topics

Monitoring Spanning Tree, on page 207

STP MSTI Configuration

This option allows you to inspect the current STP MSTI bridge instance priority configurations and change them.



MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name	00-3a-99-4d-4b-1c
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

Configuration Identification

- **Configuration Name**: The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration to share spanning trees for MSTIs (Intra-region). The name is at most 32 characters.
- **Configuration Revision**: The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

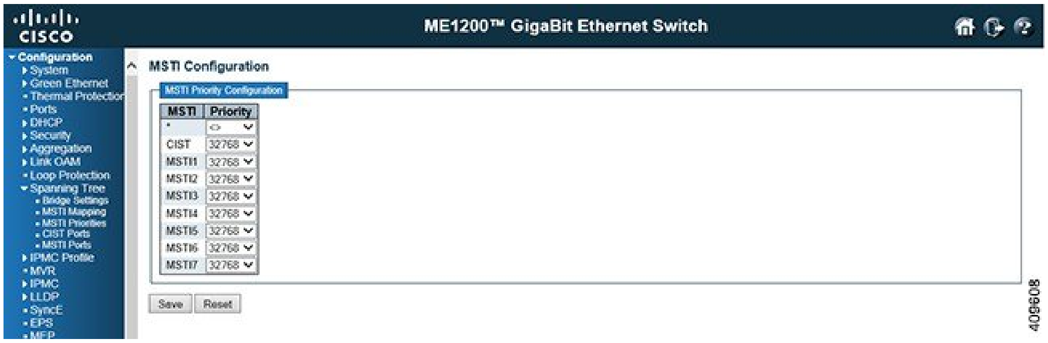
- **MSTI**: The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
- **VLANs Mapped**: The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1 and 4094) VLAN, or a range (xx-yy), each of which must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (that is, not having any VLANs mapped to it.) For example: 2, 5, 20-40.

Related Topics

Monitoring Spanning Tree, on page 207

STP MSTI Priority Configuration

This option allows you to inspect the current STP MSTI bridge instance priority configurations and change them.



MSTI Configuration

MSTI Priority Configuration

MSTI	Priority
*	<>
CIST	32768
MSTI1	32768
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768

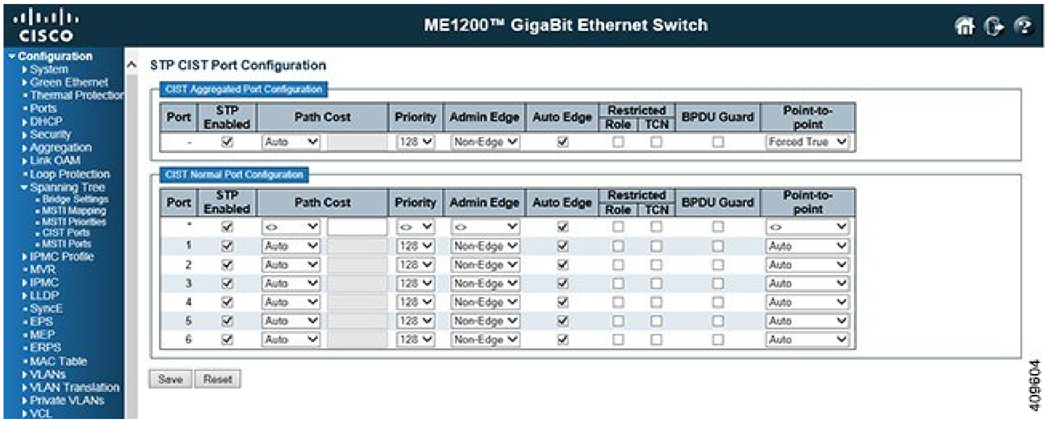
- **MSTI**: The bridge instance. The CIST is the default instance, which is always active.
- **Priority**: Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch, forms a Bridge Identifier.

Related Topics

Monitoring Spanning Tree, on page 207

STP CIST Port Configuration

This option allows you to inspect the current STP CIST port configurations and change them.



STP CIST Port Configuration

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
-	☑	Auto		128	Non-Edge	☑	□	□	□	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
*	☑	<>		<>	<>	☑	□	□	□	<>
1	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
2	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
3	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
4	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
5	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
6	☑	Auto		128	Non-Edge	☑	□	□	□	Auto

It contains settings for physical and aggregated ports.

- **Port**: The switch port number of the logical STP port.
- **STP Enabled**: Controls whether STP is enabled on this switch port.
- **Path Cost**: Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

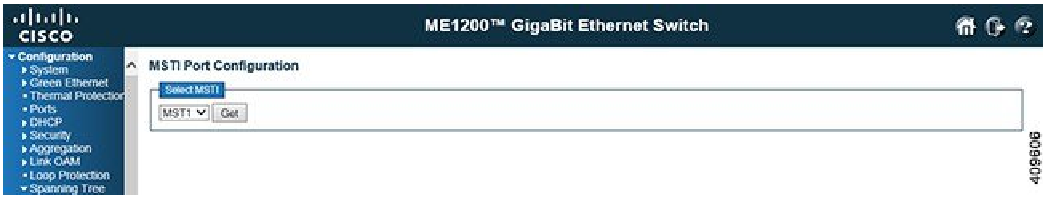
- **Priority**: Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
- *operEdge* (state flag): Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on **AdminEdge** and **AutoEdge** fields. This flag is displayed as Edge in **Monitor** > **STP Detailed Bridge Status** > **Spanning Tree**.
- **AdminEdge**: Controls whether the *operEdge* flag should start as set or cleared. (The initial *operEdge* state when a port is initialized).
- **AutoEdge**: Controls whether the bridge should enable automatic edge detection on the bridge port. This allows *operEdge* to be derived from whether BPDUs are received on the port or not.
- **Restricted Role**: If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
- **Restricted TCN**: If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

Related Topics

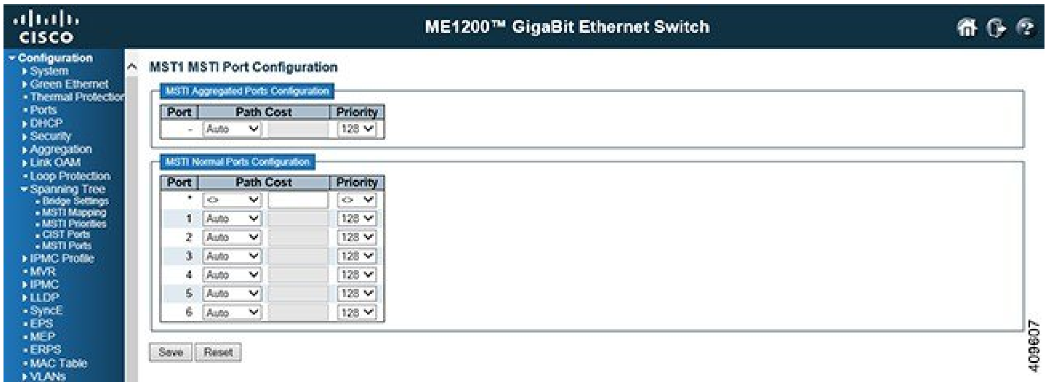
Monitoring Spanning Tree, on page 207

STP MSTI Port Configuration

This option allows you to inspect the current STP MSTI port configurations and change them.



An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. To view the actual MSTI port configuration options, shown in the below figure, select the MSTI instance and click **Get**.



MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost		Priority
-	Auto		128

MSTI Normal Ports Configuration

Port	Path Cost		Priority
*	<>		<>
1	Auto		128
2	Auto		128
3	Auto		128
4	Auto		128
5	Auto		128
6	Auto		128

This page contains MSTI port settings for physical and aggregated ports.

- **Port**: The switch port number of the corresponding STP CIST (and MSTI) port.
- **Path Cost**: Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
- **Priority**: Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

Related Topics

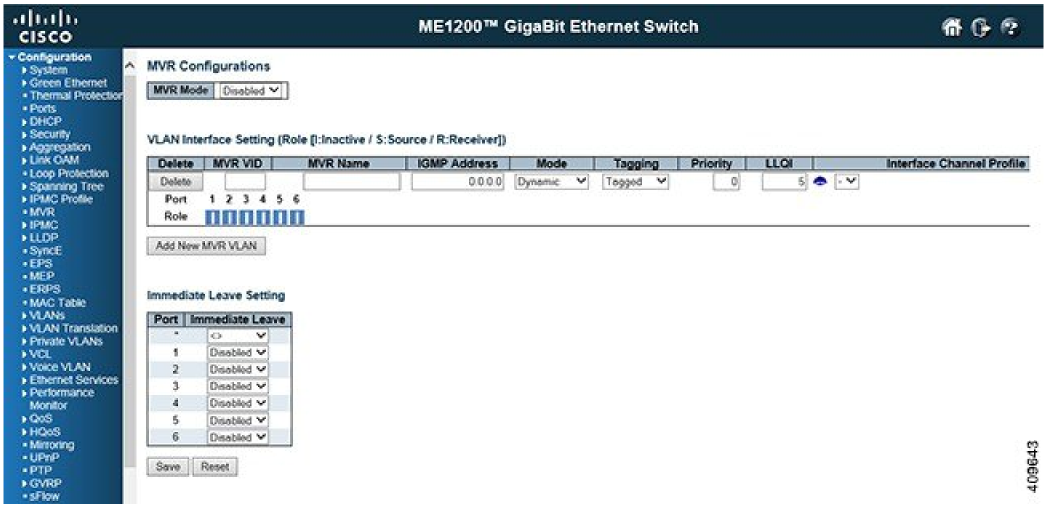
Monitoring Spanning Tree, on page 207

CHAPTER 12

Configuring MVR

MVR Configurations

This feature provides MVR related configurations. It enables multicast traffic forwarding on Multicast VLANs.



MVR Configurations

MVR Mode: Disabled

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

Delete	MVR VID	MVR Name	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile
Delete			0.0.0.0	Dynamic	Tagged	0	5	-

Port 1 2 3 4 5 6

Role I I I I I I

Immediate Leave Setting

Port	Immediate Leave
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled

In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP or MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

It is allowed to create a maximum of four MVR VLANs with corresponding channel profiles for each Multicast VLAN. The channel profile is defined by the IPMC Profile which provides the filtering conditions.

- **MVR Mode**: Enables or disables the Global MVR. The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.

- **Delete**: Check the corresponding check box to delete an entry. The selected entry will be deleted during the next Save operation.
- **MVR VID**: Specify the Multicast VLAN ID.

Note It is recommended that you avoid overlapping MVR source ports with management VLAN ports.

- **MVR Name**: MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 16. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.
- **IGMP Address**: Define the IPv4 address as source address used in IP header for IGMP control frames. The default IGMP address is not set (0.0.0.0). When the IGMP address is not set, the system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, the system uses the first available IPv4 management address.

  Otherwise, the system uses a pre-defined value. By default, this value will be 192.0.2.1.
- **Mode**: Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.
- **Tagging**: Specify whether the traversed IGMP or MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.
- **Priority**: Specify how the traversed IGMP or MLD control frames will be sent in prioritized manner. The default Priority is 0.
- **LLQI**: Define the maximum time to wait for IGMP or MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.
- **Interface Channel Profile**: When the MVR VLAN is created, select the IPMC Profile as the channel filtering condition for the specific MVR VLAN. Summary about the Interface Channel Profiling (of the MVR VLAN) will be shown by clicking the view button. Profile selected for designated interface channel is not allowed to have overlapped permit group address.
- **Navigate Profile** icon: You can use the **Navigate Profile** icon to list the rules associated with the selected profile.
- **Port**: The logical port for the settings.
- **Role**: Configure an MVR port of the designated MVR VLAN as one of the following roles.
  - Inactive: The designated port does not participate MVR operations.
  - Source: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.
  - Receiver: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.

Note It is recommended that you avoid overlapping MVR source ports with management VLAN ports.

Select the port role by clicking the Role symbol to switch the setting. I indicates Inactive; S indicates Source; R indicates Receiver. The default Role is Inactive.

- **Immediate Leave**: Enables the fast leave on the port.
- **Add new MVR VLAN**: Click this button to add a new MVR VLAN, specify the VID, and configure the new entry. Click **Save**.

Related Topics

Monitoring MVR, on page 211

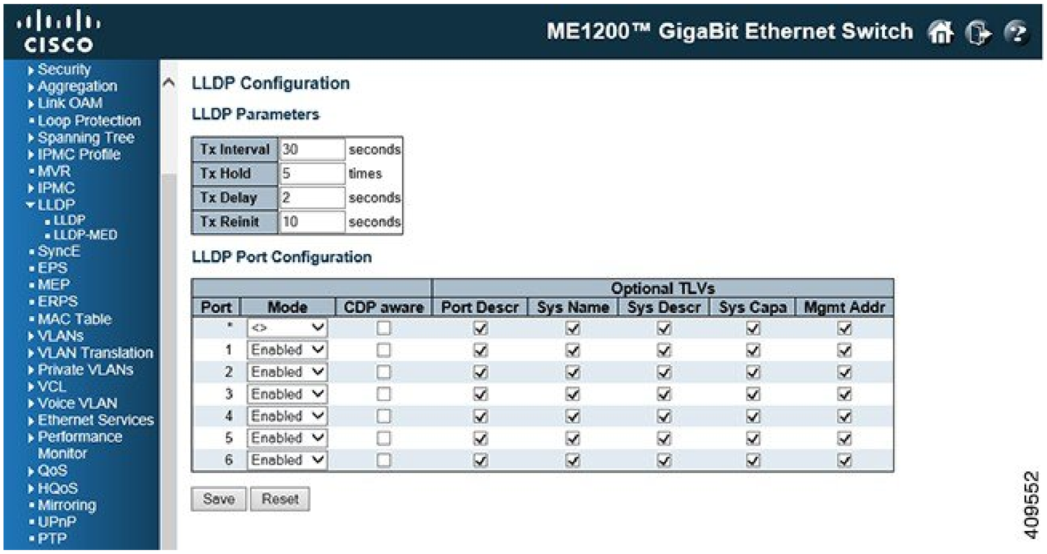
CHAPTER 13

Configuring LLDP

The LLDP feature available on the ME 1200 Web GUI allows you to configure the LLDP parameters, LLDP port, and LLDP Media.

LLDP Configuration

This option allows you to inspect and configure the current LLDP port settings.



LLDP Configuration

LLDP Parameters

Tx Interval	30	seconds
Tx Hold	5	times
Tx Delay	2	seconds
Tx Reinit	10	seconds

LLDP Port Configuration

			Optional TLVs				
Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☑	☑	☑	☑	☑
1	Enabled	☐	☑	☑	☑	☑	☑
2	Enabled	☐	☑	☑	☑	☑	☑
3	Enabled	☐	☑	☑	☑	☑	☑
4	Enabled	☐	☑	☑	☑	☑	☑
5	Enabled	☐	☑	☑	☑	☑	☑
6	Enabled	☐	☑	☑	☑	☑	☑

Save Reset

LLDP Parameters

- **Tx Interval**: The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds.
- **Tx Hold**: Each LLDP frame contains information about how long time the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.
- **Tx Delay**: If some configuration is changed (for example, the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1 - 8192 seconds.
- **Tx Reinit**: When a port is disabled, LLDP is disabled or the switch is rebooted, a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information is not valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP Port Configuration

- **Port**: The switch port number of the logical LLDP port.
- **Mode**: Select LLDP mode.
  - *Rx only*: The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.
  - *Tx only*: The switch will drop LLDP information received from neighbors, but will send out LLDP information.
  - *Disabled*: The switch will not send out LLDP information, and will drop LLDP information received from neighbors.
  - *Enabled*: The switch will send out LLDP information, and will analyze LLDP information received from neighbors.
- **CDP Aware**: Select CDP awareness. The CDP operation is restricted to decoding incoming CDP frames (The switch does not transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled. Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below. CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field. CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table. CDP TLV "Port ID" is mapped to the LLDP "Port ID" field. CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field. Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table. If all ports have CDP awareness disabled, the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled, all CDP frames are terminated by the switch.

Note When CDP awareness on a port is disabled, the CDP information is not removed immediately. It gets removed once the hold time is exceeded.

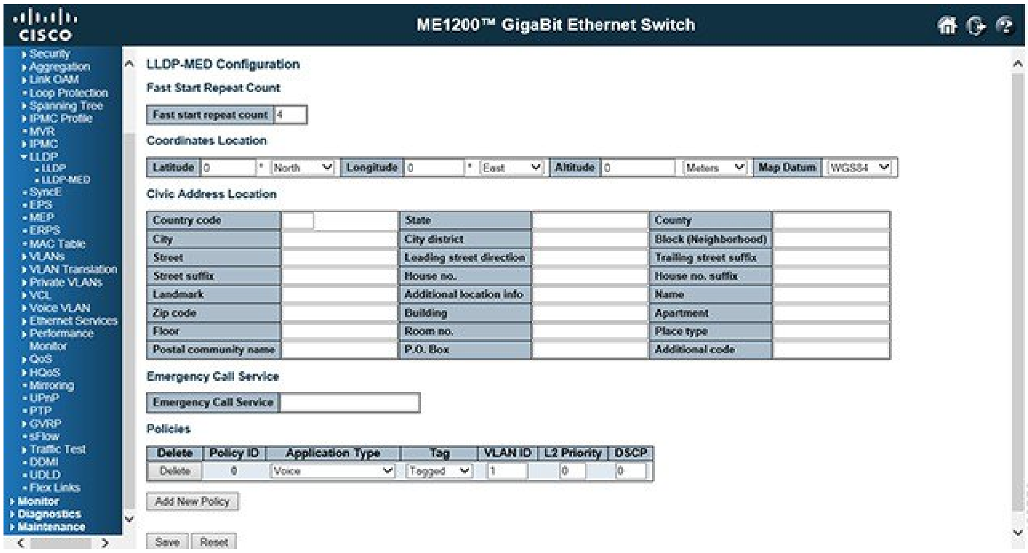
- **Port Descr**: (Optional TLV) When this check box is checked, the "port description" is included in LLDP information transmitted.
- **Sys Name**: (Optional TLV) When this check box is checked, the "system name" is included in LLDP information transmitted.
- **Sys Descr**: (Optional TLV) When this check box is checked, the "system description" is included in LLDP information transmitted.
- **Sys Capa**: (Optional TLV) When this check box is checked, the "system capability" is included in LLDP information transmitted.
- **Mgmt Addr**: (Optional TLV) When this check box is checked, the "management address" is included in LLDP information transmitted.

Related Topics

Monitoring LLDP, on page 215

LLDP Media Configuration

This option allows you to configure the LLDP-MED. This function applies to VOIP devices which support LLDP-MEP.



LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count	4

Coordinates Location

Latitude	0	° North	Longitude	0	° East	Altitude	0	Meters	Map Datum	WGS84

Civic Address Location

Country code		State		County	
City		City district		Block (Neighborhood)	
Street		Leading street direction		Trailing street suffix	
Street suffix		House no.		House no. suffix	
Landmark		Additional location info		Name	
Zip code		Building		Apartment	
Floor		Room no.		Place type	
Postal community name		P.O. Box		Additional code	

Emergency Call Service

Emergency Call Service	

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
Delete	0	Voice	Tagged	1	0	0

Add New Policy

Save Reset

Fast start repeat count

Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

With this in mind, LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network

Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors.

Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that four LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.

It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.

Coordinates Location

- **Latitude**: Latitude must be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator.
- **Longitude**: Longitude must be normalized to within 0-180 degrees with a maximum of 4 digits.It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.
- **Altitude**: Altitude must be normalized to within -32767 to 32767 with a maximum of 1 digits. It is possible to select between two altitude types (floors or meters).
    - *Meters*: Representing meters of altitude defined by the vertical datum specified.
    - *Floors*: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.
- **Map Datum**: The Map Datum is used for the coordinates given in these options:
    - *WGS84*: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.
    - *NAD83/NAVD88*: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).
    - *NAD83/MLLW*: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). The total number of characters for the combined civic address information must not exceed 250 characters. A couple of notes to the limitation of 250 characters.

Note

- More more than one civic address location is used, each of the additional civic address locations use two extra characters in addtion to the civic address location text.
- The 2 letter country code is not part of the 250 characters limitation.

Country code	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
State	National subdivisions (state, canton, region, province, prefecture).
County	County, parish, gun (Japan), district.
City	City, township, shi (Japan) - Example: Copenhagen.
City district	City division, borough, city district, ward, chou (Japan).
Block (Neighborhood)	Neighborhood, block.
Street	Street - Example: Poppelvej.
Leading street direction	Leading street direction - Example: N.
Trailing street suffix	Trailing street suffix - Example: SW.
Street suffix	Street suffix - Example: Ave, Platz.
House no.	House number - Example: 21.
House no. suffix	House number suffix - Example: A, 1/2.
Landmark	Landmark or vanity address - Example: Columbia University.
Additional location info	Additional location info - Example: South Wing.
Name	Name (residence and office occupant) - Example: Flemming Jahn.
Zip code	Postal/zip code - Example: 2791.
Building	Building (structure) - Example: Low Library.
Apartment	Unit (Apartment, suite) - Example: Apt 42.
Floor	Floor - Example: 4.

Room no.	Room number - Example: 450F.
Place type	Place type - Example: Office.
Postal community name	Postal community name - Example: Leonia.
P.O. Box	Post office box (P.O. BOX) - Example: 12345.
Additional code	Additional code - Example: 1320300003.

LLDP Media Configuration contd..

Emergency Call Service

Emergency Call Service (for example, E911 and others), such as defined by TIA or NENA. Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

- **Policies**: Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

  Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services. The network policy attributes advertised are:

  1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
  2. Layer 2 priority value (IEEE 802.1D-2004)
  3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

  This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

  1. Voice
  2. Guest Voice
  3. Softphone Voice
  4. Video Conferencing
  5. Streaming Video
  6. Control / Signalling (conditionally support a separate network policy for the media types above)

  A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

- **Delete**: Check to delete the policy. It will be deleted during the next save.
- **Policy ID**: ID for the policy. This is auto generated and is used when selecting the policies that are mapped to the specific ports.
- **Application Type**: Intended use of the application types:
    - Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
    - Voice Signalling (conditional) - for use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.
    - Guest Voice - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
    - Guest Voice Signalling (conditional) - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.
    - Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.
    - Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
    - Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
    - Video Signalling (conditional) - for use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.
- **Tag**: Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN.

    Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.

    Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.

- **VLAN ID**: VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003
- **L2 Priority**: L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.
- **DSCP**: DSCP value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.
- **Add new policy**: Click this button to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click **Save**. The number of policies supported is 32.

Port Policies Configuration

Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

- Port: The port number to which the configuration applies.
- Policy Id: The set of policies that shall apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

Related Topics

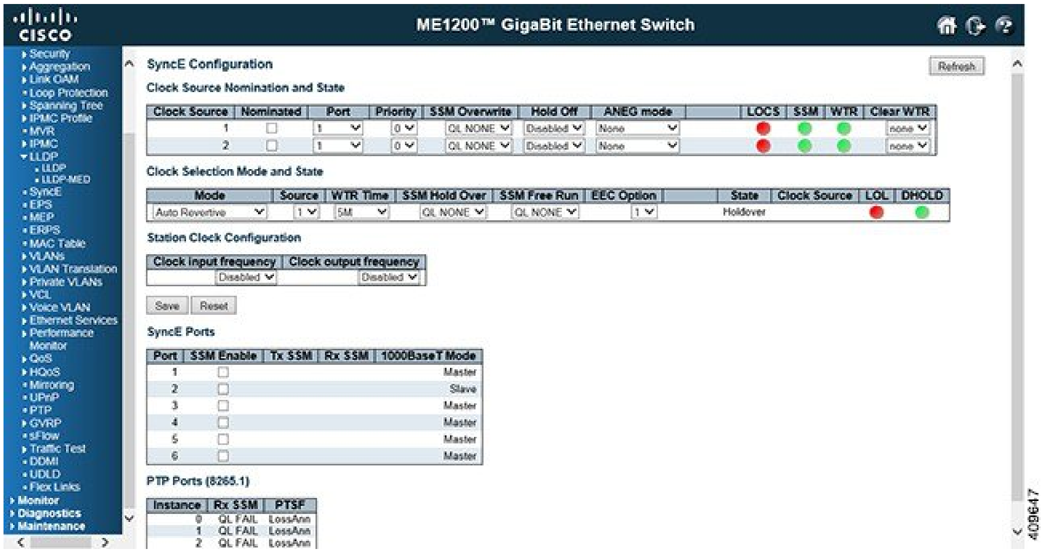
Monitoring LLDP, on page 215

CHAPTER 14

Configuring SyncE

Synchronous Ethernet Configuration

This feature allows you to inspect and configure the current SyncE port settings.



SyncE Configuration

Clock Source Nomination and State

Clock Source	Nominated	Port	Priority	SSM Overwrite	Hold Off	ANEG mode		LOCS	SSM	WTR	Clear WTR
1	□	1	0	QL NONE	Disabled	None		🔴	🟢	🟢	none
2	□	1	0	QL NONE	Disabled	None		🔴	🟢	🟢	none

Clock Selection Mode and State

Mode	Source	WTR Time	SSM Hold Over	SSM Free Run	EEC Option		State	Clock Source	LOL	DHOLD
Auto Revertive	1	5M	QL NONE	QL NONE	1		Holdover		🔴	🟢

Station Clock Configuration

Clock input frequency	Clock output frequency
Disabled	Disabled

Save Reset

SyncE Ports

Port	SSM Enable	Tx SSM	Rx SSM	1000BaseT Mode
1	□			Master
2	□			Slave
3	□			Master
4	□			Master
5	□			Master
6	□			Master

PTP Ports (8265.1)

Instance	Rx SSM	PTSF
0	QL FAIL	LossAnn
1	QL FAIL	LossAnn
2	QL FAIL	LossAnn

Clock Source Nomination and State

For each possible clock source, you can configure the following:

- **Clock Source**: This is the instance number of the clock source. This has to be referenced when selecting Manual' mode.
- **Nominated**: When a clock source is nominated, the clock output from the related PHY (Port) is enabled against the clock controller. This makes it available as a possible source in the clock selection process.

If it is supported by the actual HW configuration, The Station clock input can be nominated as a Clock Source.

- **Port**: In this drop down box, the ports that are possible to select for this clock source, is presented. The PCB104 Synce module supports 10MHz station clock input. The station clock input is indicated by a port number = 'Number of ethernet ports' + 1. The serval has a limitation that chip port 1 cannot be nominated as source 1. On the ME1200 board, it is port 3 (interface gi 1/3) .
- **Priority**: The priority for this clock source. Lowest number (0) is the highest priority. If two clock sources has the same priority, the lowest clock source number gets the highest priority in the clock selection process
- **SSM Overwrite**: A selectable clock source Quality Level (QL) to overwrite any QL received in a SSM. If QL is not Received in a SSM (SSM is not enabled on this port), the SSM Overwrite QL is used as if received. The SSM Overwrite can be set to QL_NONE, indicating that the clock source is without any know quality (Lowest compared to clock source with known quality).
- **Hold Off**: The Hold Off timer value. Active loss of clock Source will be delayed the selected amount of time. The clock selector will not change clock source if the loss of clock condition is cleared within this time.
- **ANEG mode**: This is relevant for 1000BaseT ports only. In order to recover clock from port it must be negotiated to 'Slave' mode. In order to distribute clock the port must be negotiated to 'Master' mode. This different ANEG modes can be activated on a Clock Source port:
    - *Prefer Slave*: The Port will be negotiated to 'Slave' mode if possible.
    - *Prefer Master*: The Port will be negotiated to 'Master' mode if possible.

      The selected port in 'Locked' state will always be negotiated to 'Slave' if possible.
- **LOCS**: Signal is lost on this clock source.
- **SSM**: If SSM is enabled and not received properly. Type of SSM fail will be indicated in the 'Rx SSM' field.
- **WTR**: Wait To Restore timer is active.
- **Clear WTR**: Clears the WTR timer and makes this clock source available to the clock selection process.

Synchronous Ethernet Configuration contd

Clock Selection Mode and State

The Clock Selector is only in one instance - the one who selects between the nominated clock sources.

- **Mode**: The definition of the 'best' clock source is firstly the one with the highest (QL) and secondly (the ones with equal QL) the highest priority. Clock Selector can be in different modes:
    - *Manual* : Clock selector will select the clock source stated in Source (see below). If this manually selected clock source is failing, the clock selector will go into holdover state.
    - *Manual To Selected*: Same as Manual mode where the pt. selected clock source will become Source.
    - **Auto NonRevertive**: Clock Selection of the best clock source is only done when the selected clock fails.

  - *Auto Revertive*: Clock Selection of the best clock source is constantly done.
  - *Force Hold Over*: Clock Selector is forced to Hold Over State.
  - *Force Free Run*: Clock Selector is forced to Free Run State.

- **Source**: Only relevant if Manual mode is selected (see above).
- **WTR Time**: WTR is the Wait To Restore timer value in minutes. The WTR time is activated on the falling edge of a clock source failure (in Revertive mode). This means that the clock source is first available for clock selection after WTR Time (can be cleared).
- **SSM Hold Over**: This is the transmitted SSM QL value when clock selector is in Hold Over State.
- **SSM Free Run**: This is the transmitted SSM QL value when clock selector is in Free Run State.
- **EEC Option**: The ZL30xxx based Synce modules support both EEC1 and EEC2 option. The difference is: EEC1 => DPLL bandwidth = 3,5 Hz, EEC2 => DPLL bandwidth = 0,1 Hz.
- **State**: This is indicating the state of the clock selector. Possible states are:
  - *Free Run*: There is no external clock sources to lock to (unlocked state). The Clock Selector has never been locked to a clock source long enough to calculate the hold over frequency offset to local oscillator. The frequency of this node is the frequency of the local oscillator.
  - *Hold Over*: There is no external clock sources to lock to (unlocked state). The Clock Selector has calculate the holdover frequency offset to local oscillator. The frequency of this node is hold to the frequency of the clock source previous locked to.
  - *Locked*: Clock selector is locked to the clock source indicated (See next).
  - *Top*: Clock selector is locked to Time over packets, for example, PTP (See next).
- **Clock Source**: The clock source locked to when clock selector is in locked state.
- **LOL**: Clock selector has raised the Los Of Lock alarm.
- **DHOLD**: Clock selector has not yet calculated the holdover frequency offset to local oscillator. This becomes active for about 10 s, when a new clock source is selected.

Station Clock Configuration

The SyncE module may have a Station clock input and/or a Station clock output.

- **Clock input frequency**: If supported by the Synce HW, the station clock input frequency can be configured, the possible frequencies are:1,544 MHz, 2,048 MHz or 10 MHz.
- **Clock output frequency**: If supported by the Synce HW, the station clock output frequency can be configured, the possible frequencies are:1, 544 MHz, 2, 048 MHz or 10 MHz.

SyncE Ports

For each possible port on switch.

- **Port**: The port number to configure.
- **SSM Enable**: Enable and disable of SSM functionality on this port.
- **Tx SSM**: Monitoring of the transmitted SSM QL on this port. Transmitted QL should be the Quality Level of the clock generated by this node. This means the QL of the clock source this node is locked.

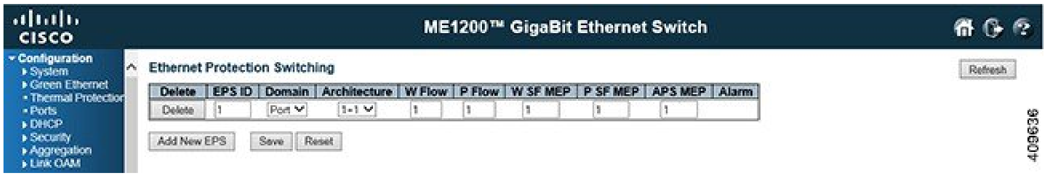
- **Rx SSM**: Monitoring of the received SSM QL on this port. If link is down on port, QL_LINK is indicated. If no SSM is received, QL_FAIL is indicated.
- **1000BaseT Mode**: If PHY is in 1000BaseT Mode then this is monitoring the master/slave mode. In order to receive clock on a port, it has to be in slave mode. To transmit clock on a port, it has to be in master mode.

CHAPTER 15

Configuring EPS

Ethernet Protection Switching

This feature allows you configure Ethernet (Linear) Protection Switch instances.



Ethernet Protection Switching

Delete	EPS ID	Domain	Architecture	W Flow	P Flow	W SF MEP	P SF MEP	APS MEP	Alarm
Delete	1	Port	1+1	1	1	1	1	1	

Add New EPS | Save | Reset

- **Delete**: Check this check box to mark an EPS for deletion in the next Save operation.
- **EPS ID**: To enter the configuration page, click the ID of an EPS.
- **Domain**:
    - *Port*: This will create an EPS in the Port Domain. 'W/P Flow' is a Port.
    - *Esp*: Future use.
    - *Evc*: This will create an EPS in the EVC Domain. 'W/P Flow' is an EVC.
    - *Mpls*: Future use.
- **Architecture**
    - *1+1*: This will create a 1+1 EPS.
    - *1:1*: This will create a 1:1 EPS.
- **W Flow**: The working flow for the EPS - See 'Domain'.
- **P Flow**: The protecting flow for the EPS - See 'Domain'.
- **W SF MEP**: The working Signal Fail reporting MEP.

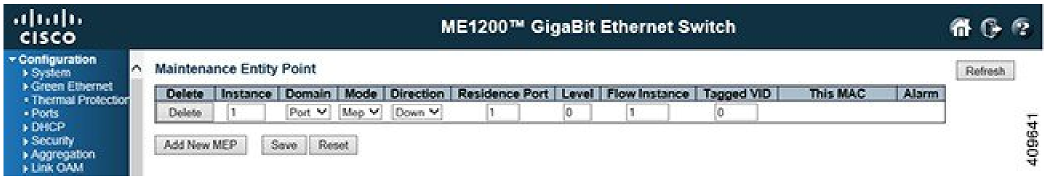
- **P SF MEP**: The protecting Signal Fail reporting MEP.
- **APS MEP**: The APS PDU handling MEP.
- **Alarm**: There is an active alarm on the EPS.

CHAPTER 16

Configuring MEP

Maintenance Entity Point

The Maintenance Entity Point instances can be configured here.



Maintenance Entity Point

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
Delete	1	Port	Mep	Down	1	0	1	0		

- **Delete**: This check box is used to mark a MEP for deletion in the next Save operation.
- **Instance**: The ID of the MEP. Click on the ID of a MEP to enter the configuration page. The range is from 1 through 100.
- **Domain**
    - *Port*: This is a MEP in the Port Domain.
    - *Evc*: This is a MEP in the EVC Domain. 'Flow Instance' is an EVC. The EVC must be created.
    - *VLAN*: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. In case of Up-MEP the VLAN must be created.
- **Mode**
    - *MEP*: This is a Maintenance Entity End Point.
    - *MIP*: This is a Maintenance Entity Intermediate Point.
- **Direction**
    - *Down*: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.
    - *Up*: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'.

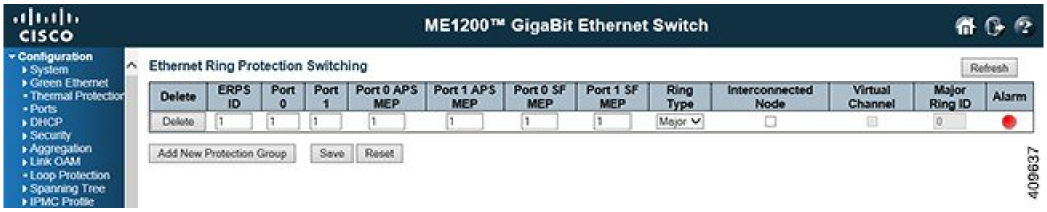
- **Residence Port**: The port where MEP is monitoring - see 'Direction'. For an EVC MEP, the port must be a port in the EVC. For a VLAN MEP, the port must be a VLAN member.
- **Level**: The MEG level of this MEP.
- **Flow Instance**: The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.
- **Tagged VID**
    - *Port MEP*: An outer C/S-tag (depending on VLAN Port Type) is added with is VID. Entering '0' means no TAG added.
    - *EVC MEP*: This is not used.
    - *VLAN MEP*: This is not used.
    - *EVC MIP*: On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active.
- **This MAC**: The MAC of this MEP - can be used by other MEP when unicast is selected (Info only)
- **Alarm**: There is an active alarm on the MEP.

CHAPTER 17

Configuring ERPS

ERPS

The ERPS instances can be configured here.



Ethernet Ring Protection Switching

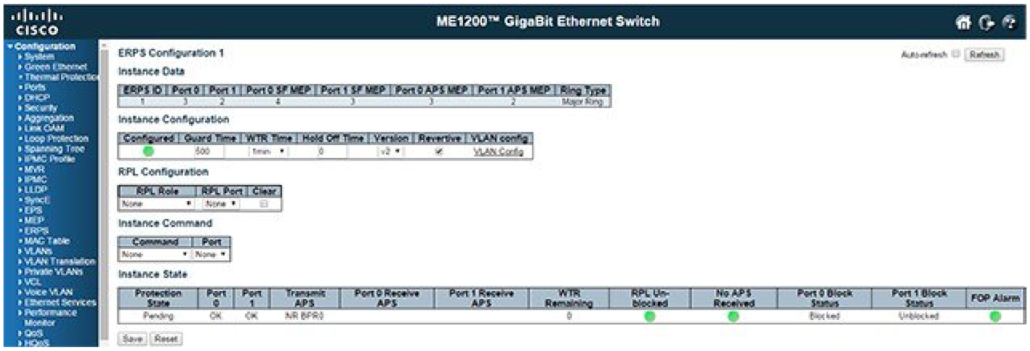
Delete	ERPS ID	Port 0	Port 1	Port 0 APS MEP	Port 1 APS MEP	Port 0 SF MEP	Port 1 SF MEP	Ring Type	Interconnected Node	Virtual Channel	Major Ring ID	Alarm
Delete	1	1	1	1	1	1	1	Major	□	□	0	●

- **Delete**: This check box is used to mark an ERPS for deletion in the next Save operation.
- **ERPS ID**: The ID of the created Protection group, It must be an integer value between 1 and 64. The maximum number of ERPS Protection Groups that can be created are 64. Click the ID of a Protection group to enter the configuration page.
- **Port 0**: This will create a Port 0 of the switch in the Ring.
- **Port 1**: This will create Port 1 of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance.
- **Port 0 SF MEP**: The Port 0 Signal Fail reporting MEP.
- **Port 1 SF MEP**: The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance.
- **Port 0 APS MEP**: The Port 0 APS PDU handling MEP.
- **Port 1 APS MEP**: The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

- **Ring Type**: Type of Protecting ring. It can be either major ring or sub-ring.
- **Interconnected Node**: Interconnected Node indicates that the ring instance is interconnected. Check the check box to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.
- **Virtual Channel**: Sub-rings can either have or not have a virtual channel on the interconnected node. This is configured using the **Virtual Channel** check box. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring does not have a virtual channel.
- **Major Ring ID**: Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.
- **Alarm**: There is an active alarm on the ERPS.

ERPS Configuration for an Instance

This option allows you to inspect and configure the current ERPS instance.



ERPS Configuration 1

Instance Data

ERPS ID	Port 0	Port 1	Port 0 SF MEP	Port 1 SF MEP	Port 0 APS MEP	Port 1 APS MEP	Ring Type
1	3	2	4	3	3	2	Major Ring

Instance Configuration

Configured	Guard Time	WTR Time	Hold Off Time	Version	Revertive	VLAN config
●	500	1min	0	v2	☑	VLAN Config

RPL Configuration

RPL Role	RPL Port	Clear
None	None	□

Instance Command

Command	Port
None	None

Instance State

Protection State	Port 0	Port 1	Transmit APS	Port 0 Receive APS	Port 1 Receive APS	WTR Remaining	RPL Un-blocked	No APS Received	Port 0 Block Status	Port 1 Block Status	FOP Alarm
Pending	OK	OK	NR BPR0			0	●	●	Blocked	Unblocked	●

Instance Data: For a description of all the fields displayed here, see ERPS, on page 91.

Instance Configuration

- **Configured**
  - Red: This ERPS is only created and has not yet been configured - is not active.
  - Green: This ERPS is configured - is active.
- **Guard Time**: Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages.

  The period of the guard timer can be configured in 10 ms steps between 10 ms and 2 seconds, with a default value of 500 ms.
- **WTR Time**: The Wait To Restore timing value to be used in revertive switching.

  The period of the WTR time can be configured by the operator in 1 minute steps between 5 and 12 minutes with a default value of 5 minutes.
- **Hold Off Time**: The timing value to be used to make persistent check on Signal Fail before switching.

  The range of the hold off timer is 0 to 10 seconds in steps of 100 ms.

- **Version**: ERPS Protocol Version - v1 or v2.
- **Revertive**: In Revertive mode, after the conditions causing a protection switch has cleared, the traffic channel is restored to the working transport entity, that is, blocked on the RPL.

  In Non-Revertive mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.
- **VLAN config**: VLAN configuration of the Protection Group. Click the **VLAN Config** link to configure VLANs for this protection group.

RPL Configuration

- **RPL Role**: It can be either RPL owner or RPL Neighbor.
- **RPL Port**: This allows you to select the east port or west port as the RPL block.
- **Clear**: If the owner has to be changed, then the **Clear** check box allows you to clear the RPL owner for that ERPS ring.

Instance Command

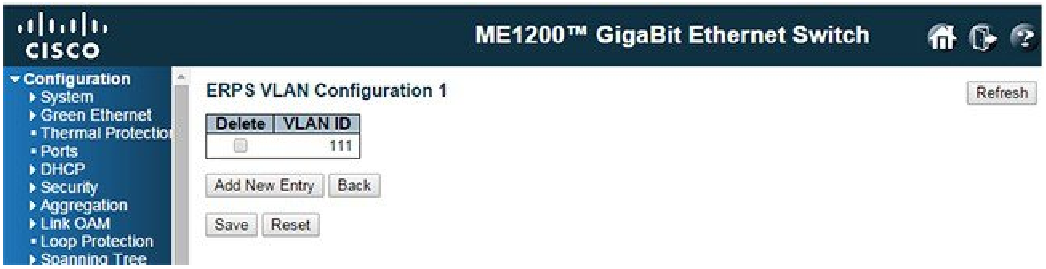
- **Command**: Administrative command. A port can be administratively configured to be in either manual switch or forced switch state.
  - *Forced Switch*: Forced Switch command forces a block on the ring port where the command is issued.
  - *Manual Switch*: In the absence of a failure or FS, Manual Switch command forces a block on the ring port where the command is issued.
  - *Clear*: The Clear command is used for clearing an active local administrative command (for example, Forced Switch or Manual Switch).
- **Port**: Port selection - Port0 or Port1 of the Protection Group on which the command is applied.

Instance State

- **Protection State**: ERPS state according to State Transition Tables in G.8032.
- **Port 0**
  - *OK*: State of East port is ok.
  - *SF*: State of East port is Signal Fail.
- **Port 1**
  - *OK*: State of West port is ok.
  - *SF*: State of West port is Signal Fail.
- **Transmit APS:** The transmitted APS according to State Transition Tables in G.8032.
- **Port 0 Receive APS**: The received APS on Port 0 according to State Transition Tables in G.8032.
- **Port 1 Receive APS**: The received APS on Port 1 according to State Transition Tables in G.8032.
- **WTR Remaining**: Remaining WTR timeout in milliseconds.

- **RPL Un-blocked**: APS is received on the working flow.
- **No APS Received**: RAPS PDU is not received from the other end.
- **Port 0 Block Status**: Block status for Port 0 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.
- **Port 1 Block Status**: Block status for Port 1 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.
- **FOP Alarm**: Failure of Protocol Defect(FOP) status. If FOP is detected, red LED glows; else green LED glows.

ERPS VLAN Configuration



ERPS VLAN Configuration 1

Delete	VLAN ID
□	111

- **Delete**: To delete a VLAN entry, check this check box. The entry will be deleted during the next Save operation.
- **VLAN ID**: Indicates the ID of this particular VLAN.
- **Add New Entry**: Click this button to add a new VLAN ID. Legal values for a VLAN ID are 1 through 4095.

The VLAN is enabled when you click **Save**. A VLAN without any port members will be deleted when you click **Save**.

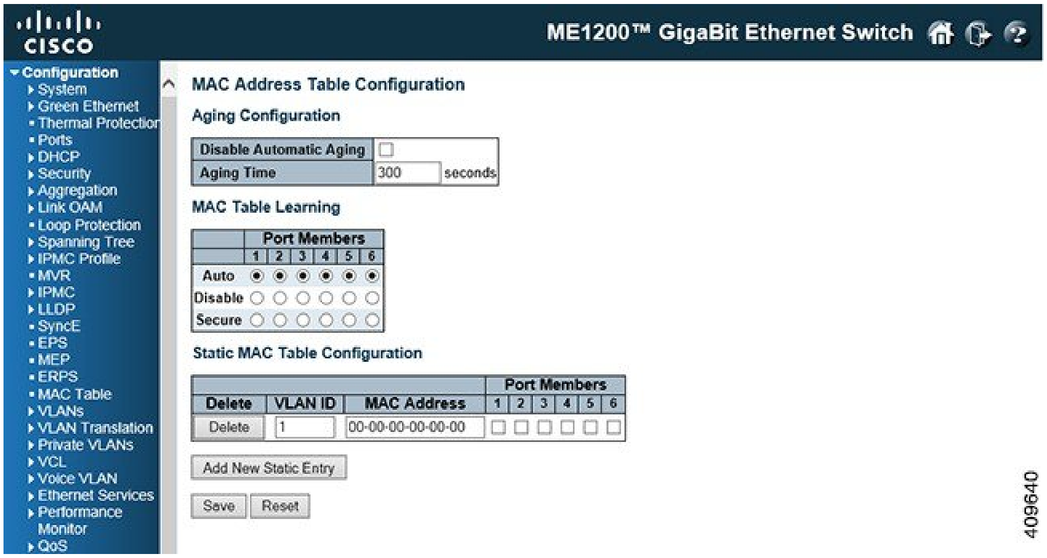
The **Delete** check box can be used to undo the addition of new VLANs.

CHAPTER 18

Configuring MAC Table

MAC Address Table Configuration

This feature allows you to set the MAC Address Table configuration. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.



MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	□	
Aging Time	300	seconds

MAC Table Learning

	Port Members					
	1	2	3	4	5	6
Auto	●	●	●	●	●	●
Disable	○	○	○	○	○	○
Secure	○	○	○	○	○	○

Static MAC Table Configuration

			Port Members					
Delete	VLAN ID	MAC Address	1	2	3	4	5	6
Delete	1	00-00-00-00-00-00	□	□	□	□	□	□

Add New Static Entry

Save Reset

Aging Configuration

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging. Configure aging time by entering a value in seconds.

To disable the automatic aging of dynamic entries, check the **Disable Automatic Aging** checkbox.

MAC Table Learning

If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.

Each port can do learning based upon the following settings:

- **Auto**: Learning is done automatically as soon as a frame with unknown SMAC is received.
- **Disable**: No learning is done.
- **Secure**: Only static MAC entries are learned, all other frames are dropped.

Note Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch through the serial interface.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. It is sorted first by VLAN ID and then by MAC address.

- **Delete**: Check to delete the entry. It will be deleted during the next save.
- **VLAN ID**: The VLAN ID of the entry.
- **MAC Address**: The MAC address of the entry.
- **Port Members**: Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
- **Add New Static Entry**: Click this button to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click **Save**.

Related Topics

Monitoring MAC Table, on page 233

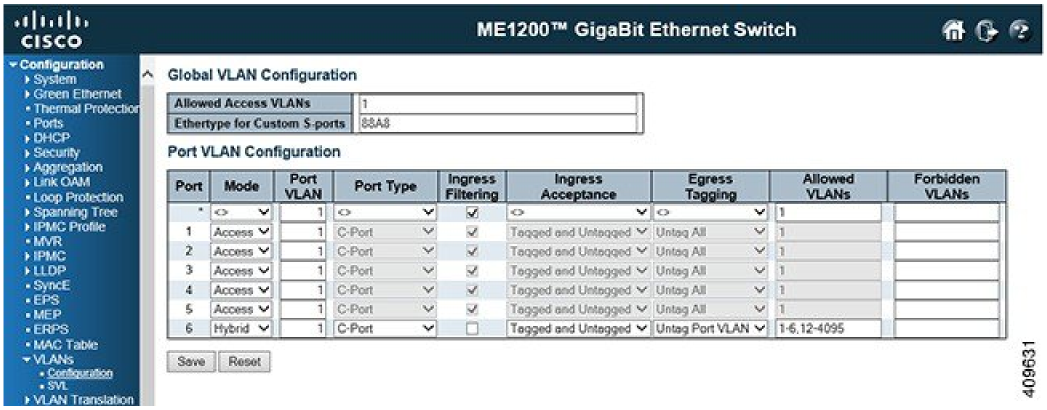
CHAPTER 19

Configuring VLANs

The VLANs feature available on the ME 1200 Web GUI allows you to set the Global VLAN and Port VLAN configurations.

VLAN Configuration

This option allows for controlling VLAN configuration on the switch.It is divided into a global section and a per-port configuration section.



Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Hybrid	1	C-Port	□	Tagged and Untagged	Untag Port VLAN	1-6,12-4095	

Global VLAN Configuration

- **Allowed Access VLANs**: This field shows the allowed Access VLANs, that is, it only affects ports configured as Access ports. Ports in other modes are members of all VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound

  The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13, 200, 300. Spaces are allowed in between the delimiters.

- **Ethertype for Custom S-ports**: This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.

Port VLAN Configuration

- **Port**: This is the logical port number of this row.
- **Mode**: The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below.

  Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question.

  Grayed out fields show the value that the port will get when the mode is applied.

  - *Access*: Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:
    - Member of exactly one VLAN, the Port VLAN (also called as Access VLAN), which by default is 1.
    - Accepts untagged and C-tagged frames.
    - Discards all frames that are not classified to the Access VLAN.
    - On egress all frames are transmitted untagged.
  - *Trunk*: Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:
    - By default, a trunk port is member of all VLANs (1-4095).
    - The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs.
    - Frames classified to a VLAN that the port is not a member of are discarded.
    - By default, all frames but frames classified to the Port VLAN (also called as Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress.
    - Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress.
  - *Hybrid*: Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:
    - Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware.
    - Ingress filtering can be controlled.
    - Ingress acceptance of frames and configuration of egress tagging can be configured independently.
- **Port VLAN**: Determines the port's VLAN ID (also called as PVID). Allowed VLANs are in the range 1 through 4095, default being 1.

On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).

On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN. The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.

- **Port Type**: Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.
    - *Unaware*: On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.
    - *C-Port*: On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag.
    - *S-Port*: On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.
    - *S-Custom-Port*: On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.

- **Ingress Filtering**: Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled. If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.

- **Ingress Acceptance**: Hybrid ports allow for changing the type of frames that are accepted on ingress.
    - *Tagged and Untagged*: Both tagged and untagged frames are accepted.
    - *Tagged Only*: Only tagged frames are accepted on ingress. Untagged frames are discarded.
    - *Untagged Only*: Only untagged frames are accepted on ingress. Tagged frames are discarded.

- **Egress Tagging**: Ports in Trunk and Hybrid mode may control the tagging of frames on egress.
    - *Untag Port VLAN*: Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.
    - *Tag All*: All frames, whether classified to the Port VLAN or not, are transmitted with a tag.
    - *Untag All*: All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.

- **Allowed VLANs**: Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to 1-4095.

The field may be left empty, which means that the port will not become member of any VLANs.

- **Forbidden VLANs**: A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field.

  By default, the field is left blank, which means that the port may become a member of all possible VLANs.

Related Topics

Monitoring VLANs, on page 235

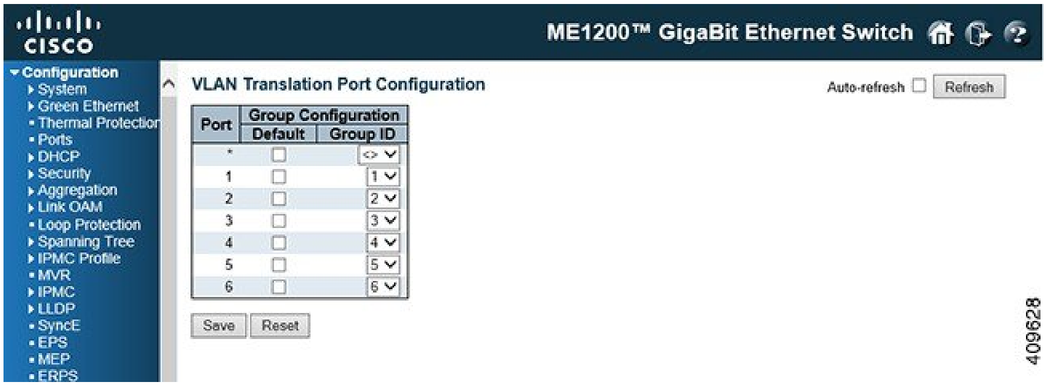
CHAPTER 20

Configuring VLAN Translation

The VLAN Translation feature available on the ME 1200 Web GUI allows you to configure the VLAN Translation Port and the VLAN Translation Mappings.

VLAN Translation Port Configuration

This option allows you to configure switch Ports to use a given VLAN Translation Mapping Group. This will enable all VLAN Translation mappings of that group (if any) on the selected switch port.



VLAN Translation Port Configuration

Port	Group Configuration	
	Default	Group ID
*	□	<>
1	□	1
2	□	2
3	□	3
4	□	4
5	□	5
6	□	6

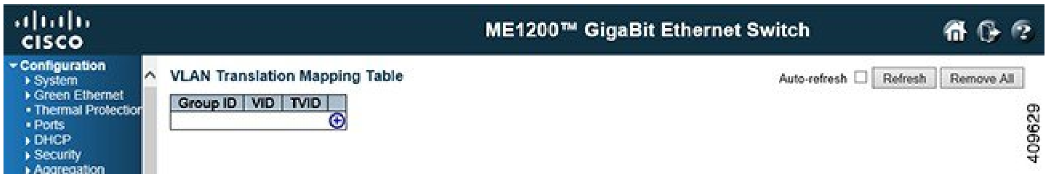
The displayed settings are:

- **Port**: The Port column shows the list of ports for which you can configure the VLAN Translation Mapping Group.
- **Default**: To set the switch port to use the default VLAN Translation Group click the checkbox and press Save.
- **Group ID**: The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use a number of VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number

of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from 1 to 6.

Note By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1.

VLAN Translation Mapping Table



VLAN Translation Mapping Table

Group ID	VID	TVID

This option allows you to create mappings of VLANs to Translated VLANs and organize these mappings into global Groups.

- **Group ID**: The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use a number of VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from 1 to 6.

  Note By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1.

- **VID**: Indicates the VLAN of the mapping (that is, 'source' VLAN). A valid VLAN ID ranges from 1 to 4095.
- **TVID**: Indicates the VLAN ID to which VLAN ID of an ingress frame will be translated to (granted that the mapping is enabled on the ingress port that the frame arrived at). A valid VLAN ID ranges from 1 to 4095.
- Modification icons: You can modify each VLAN Translation mapping in the table using the following icons:
  - **Edit Mapping** icon: Edits the mapping row.
  - **Delete Mapping** icon: Deletes the mapping.
  - **Add New Mapping** icon: Adds a new mapping.

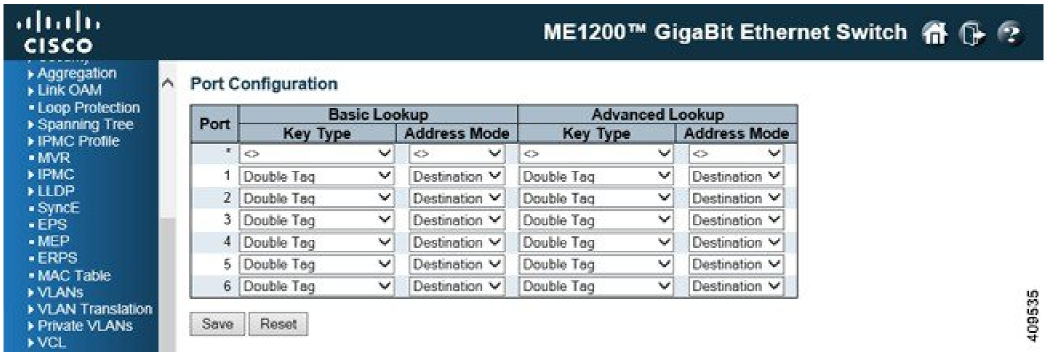
CHAPTER 21

Configuring Ethernet Services

The Ethernet Services feature available on the ME 1200 Web GUI allows you to configure the EVC port, EVC L2CP, EVC bandwidth, and EVC Control List.

EVC Port Configuration

This option displays current EVC port configurations. The settings can also be configured here.



Port Configuration

Port	Basic Lookup		Advanced Lookup	
	Key Type	Address Mode	Key Type	Address Mode
*	<>	<>	<>	<>
1	Double Tag	Destination	Double Tag	Destination
2	Double Tag	Destination	Double Tag	Destination
3	Double Tag	Destination	Double Tag	Destination
4	Double Tag	Destination	Double Tag	Destination
5	Double Tag	Destination	Double Tag	Destination
6	Double Tag	Destination	Double Tag	Destination

- **Port**: The logical port for the settings contained in the same row.
- Basic **Key Type**: The key type specifying the key generated for frames received on the port. The allowed values are:
  - *Normal*: Half key, matches outer tag, SIP/DIP and SMAC/DMAC.
  - *Double Tag*: Quarter key, matches inner and outer tag.

  - *IP Address*: Half key, matches inner and outer tag, SIP and DIP. For non-IP frames, match outer tag only.
  - *MAC and IP Address*: Full key, matches inner and outer tag, SMAC, DMAC, SIP, and DIP.

    Filtering on DMAC type (unicast or multicast or broadcast) is supported for any key type.

- Basic **Address Mode**: The IP/MAC address mode that specifies whether the EVC classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses. This parameter is only used when the key type is Normal. The allowed values are:
  - *Source*: Enables SMAC/SIP matching.
  - *Destination*: Enables DMAC/DIP matching.

- Advanced **Key Type**: The advanced key type specifying the key generated for the second lookup. The allowed values are:
  - *Normal*: Half key, match outer tag, SIP/DIP and SMAC/DMAC.
  - *Double Tag*: Quarter key, match inner and outer tag.
  - *IP Address*: Half key, match inner and outer tag, SIP, and DIP. For non-IP frames, match outer tag only.
  - *MAC and IP Address*: Full key, match inner and outer tag, SMAC, DMAC, SIP and DIP.

    Filtering on DMAC type (unicast/multicast/broadcast) is supported for any key type.

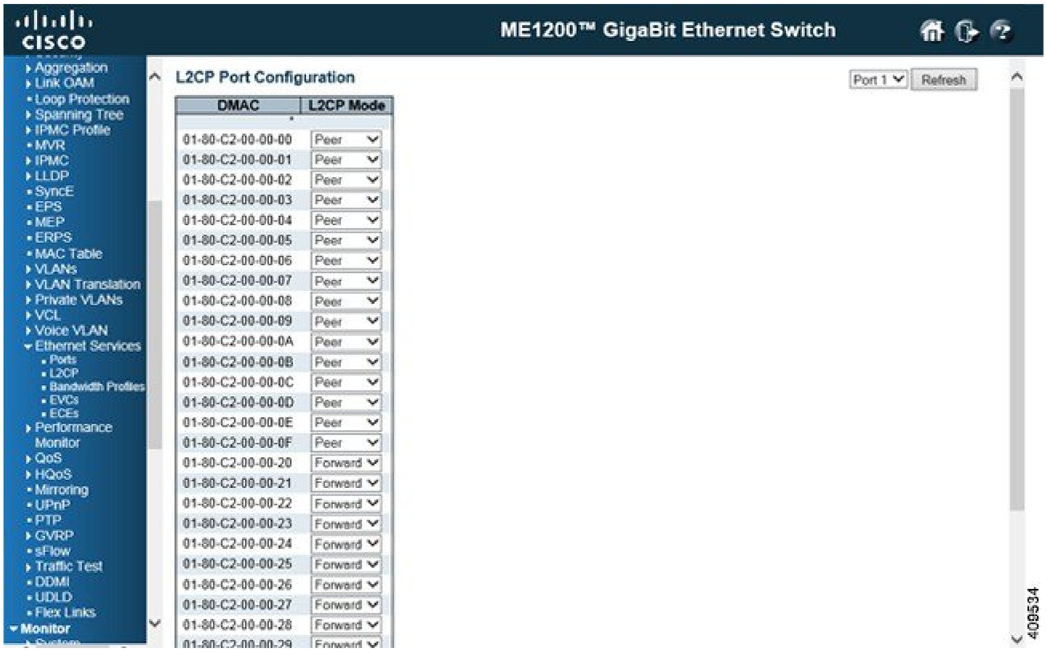
- Advanced **Address Mode**: The advanced IP/MAC address mode specifying for the second lookup. This parameter is only used when the key type is Normal. The allowed values are:
  - *Source*: Enables SMAC/SIP matching.
  - *Destination*: Enables DMAC/DIP matching.

Related Topics

Port Configuration, on page 12
Monitoring Ethernet Services, on page 223

EVC L2CP Configuration

This option displays current EVC L2CP configurations. The settings can also be configured here.



L2CP Port Configuration

DMAC	L2CP Mode
01-80-C2-00-00-00	Peer
01-80-C2-00-00-01	Peer
01-80-C2-00-00-02	Peer
01-80-C2-00-00-03	Peer
01-80-C2-00-00-04	Peer
01-80-C2-00-00-05	Peer
01-80-C2-00-00-06	Peer
01-80-C2-00-00-07	Peer
01-80-C2-00-00-08	Peer
01-80-C2-00-00-09	Peer
01-80-C2-00-00-0A	Peer
01-80-C2-00-00-0B	Peer
01-80-C2-00-00-0C	Peer
01-80-C2-00-00-0D	Peer
01-80-C2-00-00-0E	Peer
01-80-C2-00-00-0F	Peer
01-80-C2-00-00-20	Forward
01-80-C2-00-00-21	Forward
01-80-C2-00-00-22	Forward
01-80-C2-00-00-23	Forward
01-80-C2-00-00-24	Forward
01-80-C2-00-00-25	Forward
01-80-C2-00-00-26	Forward
01-80-C2-00-00-27	Forward
01-80-C2-00-00-28	Forward
01-80-C2-00-00-29	Forward

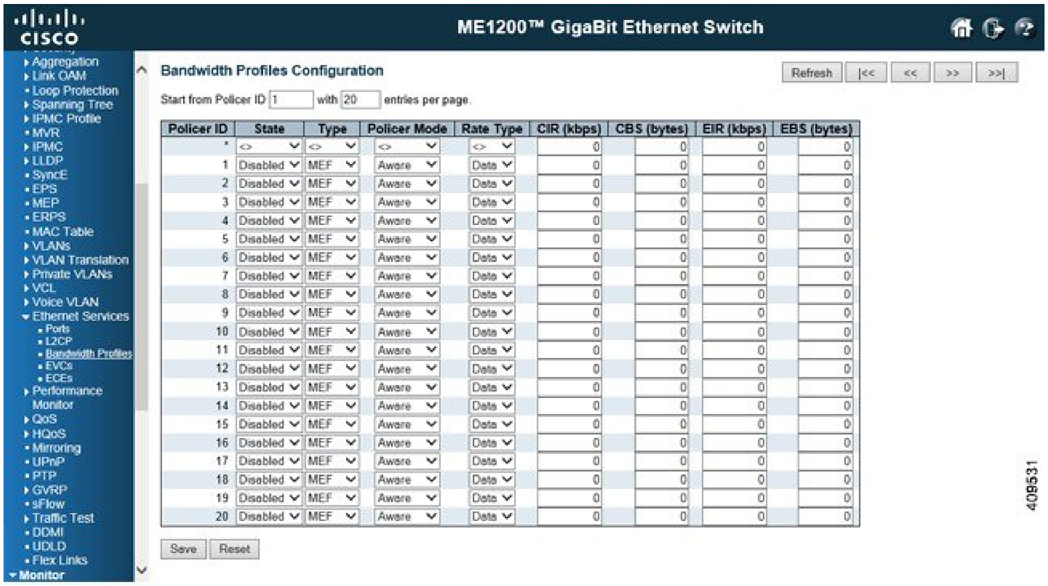
- **DMAC**: The destination BPDU MAC addresses (01-80-C2-00-00-0X) and GARP (01-80-C2-00-00-2X) MAC addresses for the settings contained in the same row.
- **L2CP Mode**: The L2CP mode for the specific port. The possible values are:
    - *Peer*: Redirects to CPU to allow 18 peering/tunneling/discard depending on ECE and protocol configuration.
    - *Forward*: Allows to 20 peer/forward/tunnel/discard depending on ECE and protocol configuration.
    - *Discard*: Drops frame.

Related Topics

Monitoring Ethernet Services, on page 223

EVC Bandwidth Profile Configuration

This page displays current EVC ingress bandwidth profile configurations. These policers may be used to limit the traffic received on UNI ports. The settings can also be configured here.



Bandwidth Profiles Configuration

Start from Policer ID 1 with 20 entries per page.

Policer ID	State	Type	Policer Mode	Rate Type	CIR (kbps)	CBS (bytes)	EIR (kbps)	EBS (bytes)
*	<>	<>	<>	<>	0	0	0	0
1	Disabled	MEF	Aware	Data	0	0	0	0
2	Disabled	MEF	Aware	Data	0	0	0	0
3	Disabled	MEF	Aware	Data	0	0	0	0
4	Disabled	MEF	Aware	Data	0	0	0	0
5	Disabled	MEF	Aware	Data	0	0	0	0
6	Disabled	MEF	Aware	Data	0	0	0	0
7	Disabled	MEF	Aware	Data	0	0	0	0
8	Disabled	MEF	Aware	Data	0	0	0	0
9	Disabled	MEF	Aware	Data	0	0	0	0
10	Disabled	MEF	Aware	Data	0	0	0	0
11	Disabled	MEF	Aware	Data	0	0	0	0
12	Disabled	MEF	Aware	Data	0	0	0	0
13	Disabled	MEF	Aware	Data	0	0	0	0
14	Disabled	MEF	Aware	Data	0	0	0	0
15	Disabled	MEF	Aware	Data	0	0	0	0
16	Disabled	MEF	Aware	Data	0	0	0	0
17	Disabled	MEF	Aware	Data	0	0	0	0
18	Disabled	MEF	Aware	Data	0	0	0	0
19	Disabled	MEF	Aware	Data	0	0	0	0
20	Disabled	MEF	Aware	Data	0	0	0	0

- Start Policer ID: The start Policer ID for displaying the table entries. The allowed range is from 1 through 1022.
- Number of Entries: The number of entries per page. The allowed range is from 2 through 1022.
- **Policer ID**: The Policer ID is used to identify one of the 1022 policers.
- **State**: The administrative state of the bandwidth profile. The allowed values are:
  - ***Enabled***: The bandwidth profile enabled.
  - ***Disabled***: The bandwidth profile is disabled.
- **Type**: The policer type of the bandwidth profile. The allowed values are:
  - *MEF*: MEF ingress bandwidth profile.
  - *Single*: Single bucket policer.
- **Policer Mode**: The color mode of the bandwidth profile. The allowed values are:
  - *Coupled*: Color-aware mode with coupling enabled.
  - *Aware*: Color-aware mode with coupling disabled.
- **Rate Type**: The rate type of the bandwidth profile. The allowed values are:
  - *Data*: Specifies that this bandwidth profile operates on data rate.
  - *Line*: Specifies that this bandwidth profile operates on line rate.
- **CIR**: The Committed Information Rate of the bandwidth profile. The allowed range is from 0 through 10000000 kilobit per second.
- **CBS**: The Committed Burst Size of the bandwidth profile. The allowed range is from 0 through 100000 bytes.

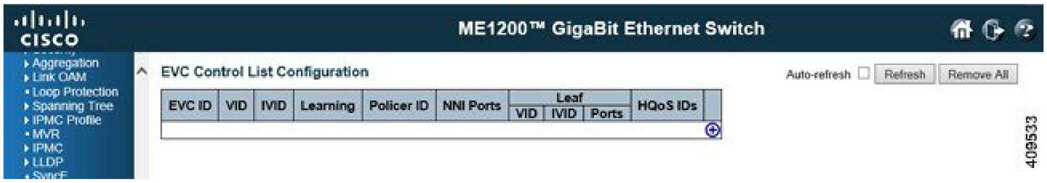
- **EIR**: The Excess Information Rate for MEF type bandwidth profile. The allowed range is from 0 through 10000000 kilobit per second.
- **EBS**: The Excess Burst Size for MEF type bandwidth profile. The allowed range is from 0 through 100000 bytes.

Related Topics

Bandwidth Profiles Configuration, on page 12
Monitoring Ethernet Services, on page 223

EVC Control List Configuration

This option displays current EVC configurations. On this system, only Provider Bridge based EVCs are supported.



EVC Control List Configuration

EVC ID	VID	IVID	Learning	Policer ID	NNI Ports	Leaf			HQoS IDs
						VID	IVID	Ports	

- **EVC ID**: The EVC ID identifies the EVC. The range is from 1 through 1024.
- **VID**: The VLAN ID in the PB network. It may be inserted in a C-tag, S-tag, or S-custom tag depending on the NNI port VLAN configuration. The range is from 0 through 4095.
- **IVID**: The internal or classified VLAN ID in the PB network. The range is from 1 through 4095
- **Learning**: The learning mode for the EVC controls whether source MAC addresses are learned for frames matching the EVC. Learning may be disabled if the EVC only includes two UNI or NNI ports. The possible values are:
  - *Enabled*: Learning is enabled (MAC addresses are learned).
  - *Disabled*: Learning is disabled (MAC addresses are not learned).
- **Policer ID**: The ingress bandwidth profile mode for the EVC. The possible values are:
  - *Specific*: The range is from 1 through 1022.
  - *Discard*: All received frames are discarded for the EVC.
  - *None*: None bandwidth profile for the EVC.
- **NNI Ports**: The list of Network to Network Interfaces for the EVC.
- **Leaf VID**: The leaf VLAN ID used in the outer tag for the EVC.
- **Leaf IVID**: The leaf internal classified VLAN ID for the EVC.
- **Leaf Ports**: The list of leaf ports for the EVC.
- **HQoS IDs**: The list of HQoS entries mapped to the EVC ports and a link to configure the mappings.

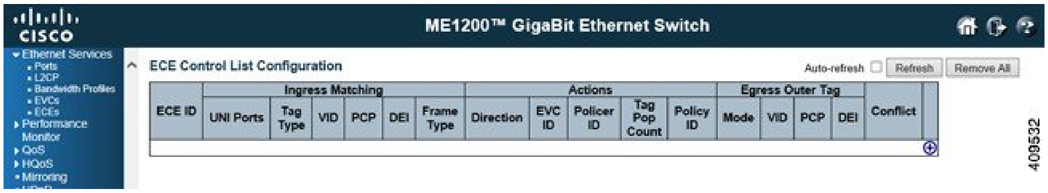
- Modification icons: You can modify each EVC in the table using the following icons:
    - **Edit EVC** icon: Edits the EVC row.
    - **Delete EVC** icon: Deletes the EVC.
    - **Add New EVC** icon: Adds a new EVC.

Related Topics

Monitoring Ethernet Services, on page 223

ECE Control List Configuration

This option displays the current EVC Control Entries (ECEs). The settings can also be configured here.



ECE Control List Configuration

ECE ID	Ingress Matching						Actions					Egress Outer Tag				Conflict
	UNI Ports	Tag Type	VID	PCP	DEI	Frame Type	Direction	EVC ID	Policer ID	Tag Pop Count	Policy ID	Mode	VID	PCP	DEI	

ECE ID: The ECE ID identifies the ECE. Unique ECE IDs are automatically assigned to ECEs added. The range is from 1 through 1024.

Ingress Matching

- **UNI Ports**: The list of User Network Interfaces for the ECE.
- **Tag Type**: The tag type for the ECE. The possible values are:
    - ◦ *Any*: The ECE matches both tagged and untagged frames.
    - ◦ *Untagged*: The ECE matches untagged frames only.
    - ◦ *C-Tagged*: The ECE matches custom tagged frames only.
    - ◦ *S-Tagged*: The ECE matches service tagged frames only.
    - ◦ *Tagged*: The ECE matches tagged frames only.
- **VID**: The VLAN ID for the ECE. It is only significant if the tag type *Tagged* is selected. The possible values are:
    - *Specific*: The range is from 1 through 4095.
    - *Any*: The ECE matches any VLAN ID.
- **PCP**: The PCP value for the ECE. It is only significant if the tag type *Tagged* is selected. The possible values are:
    - *Specific*: The ECE matches a specific PCP in the range 0 through 7.
    - *Range*: The ECE matches PCP values in the selected range 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.

    - *Any*: The ECE matches any PCP value.

- **DEI**: The DEI value for the ECE. It is only significant if the tag type *Tagged* is selected. The possible values are: 0, 1, or Any.
- **Frame Type**: The frame type for the ECE. The possible values are:
    - *Any*: The ECE matches any frame type.
    - *IPv4*: The ECE matches IPv4 frames only.
    - *IPv6*: The ECE matches IPv6 frames only.
    - *Ethernet Type*: The ECE matches Ethernet type frames only.
    - *LLC*: The ECE matches LLC frames only.
    - *SNAP*: The ECE matches SNAP frames only.
    - *L2CP*: The ECE matches L2CP frames only.

Actions

- **Direction**: The EVCs and ECEs are used to setup flows in one or both directions as determined by the ECE Direction parameter. If the ECE is bidirectional, the ingress rules of the NNI ports is set up to match the traffic being forwarded to NNI ports. Possible values are:
    - *Both*: Bidirectional.
    - *UNI-to-NNI*: Unidirectional from UNI to NNI.
    - *NNI-to-UNI*: Unidirectional from NNI to UNI.
- **EVC ID**: The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. Possible values are:
    - *Specific*: The range is from 1 through 1024.
    - *None*: The ECE does not map to an EVC.
- **Policer ID**: The ingress bandwidth profile mode for the ECE. The possible values are:
    - *Specific*: The range is from 1 through 1022.
    - *Discard*: All received frames are discarded for the ECE.
    - *None*: All received frames are forwarded for the ECE.
- **Tag Pop Count**: The ingress tag pop count for the ECE. The possible range is from 0 through 2.
- **Policy ID**: The ACL Policy ID for the ECE. The range is from 0 through 63.

Egress Outer Tag

- **Outer Tag Mode**: The outer tag for nni-to-uni direction for the ECE. The possible values are:
    - ◦ *Enable*: Enable outer tag for nni-to-uni direction for the ECE.
    - ◦ *Disable*: Disable outer tag for nni-to-uni direction for the ECE.

- **Outer Tag VID**: The EVC outer tag VID for UNI ports. The range is from 0 through 4095.
- **Outer Tag PCP**: The outer tag PCP mode for the ECE. The possible values are:
    - *Classified*: The outer tag PCP Mode is classified.
    - *Mapped*: The outer tag PCP Mode is based on mapped (QOS, DP) or the fixed PCP value from 0 through 7.
- **Outer Tag DEI**: The outer tag DEI mode for the ECE. The possible values are:
    - *Classified*: The outer tag DEI mode is classified.
    - *Drop Precedence*: The outer tag DEI mode is drop precedence or the fixed DEI value 0 or 1.
- **Conflict**: Indicates the hardware status of the specific ECE. The specific ECE is not applied to the hardware due to hardware limitations.
- Modification icons: You can modify each EVC Control Entry (ECE) in the table using the following icons:
    - **Insert new ECE before this ECE** icon: Inserts a new ECE before the current row.
    - **Edit ECE** icon: Edits the ECE row.
    - **Move ECE up** icon: Moves the ECE up the list.
    - **Move ECE down** icon: Moves the ECE down the list.
    - **Delete ECE** icon: Deletes the ECE.
    - **Add ECE to end of list** icon: The lowest plus sign adds a new entry at the bottom of the ECE listings.

Related Topics

Monitoring Ethernet Services, on page 223

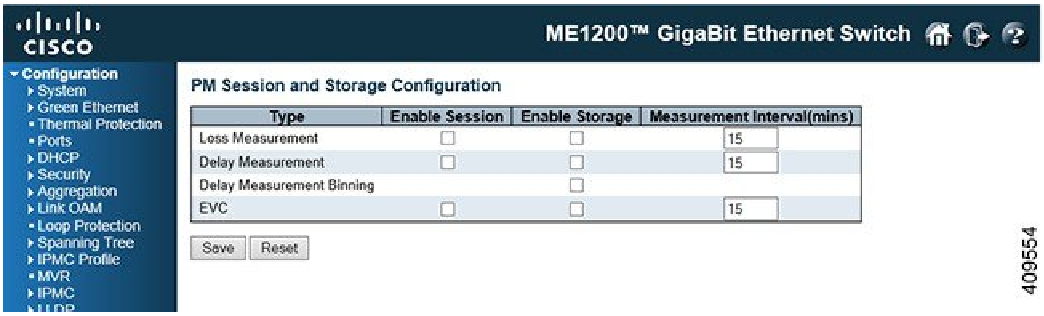
CHAPTER 22

Configuring Performance Monitor

The Performance Monitor feature available on the ME 1200 Web GUI allows you to configure the Performance Monitor and the Performance Monitor Transfer.

Performance Monitor Configuration

This option displays current Performance Monitor (PM) configurations. You can also configure new settings.



PM Session and Storage Configuration

Type	Enable Session	Enable Storage	Measurement Interval(mins)
Loss Measurement	□	□	15
Delay Measurement	□	□	15
Delay Measurement Binning		□	
EVC	□	□	15

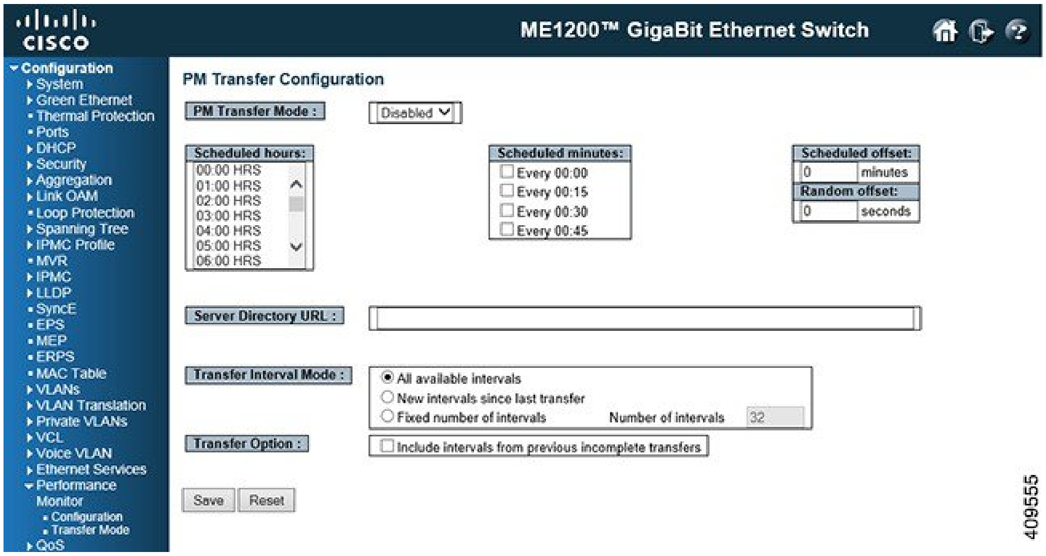
- **Type**: The data type of the PM.
- **Enable Session**: Enables or disables the PM session.
- **Enable Storage**: Enables or disables the PM storage.
- **Measurement Interval(mins)**: The measurement interval for the PM.

Related Topics

Monitoring Performance Monitor, on page 225

Performance Monitor Transfer Configuration

This option displays current PM transfer configurations. You can also configure new settings.



PM Transfer Configuration

PM Transfer Mode : Disabled

Scheduled hours: 00:00 HRS, 01:00 HRS, 02:00 HRS, 03:00 HRS, 04:00 HRS, 05:00 HRS, 06:00 HRS

Scheduled minutes:
□ Every 00:00
□ Every 00:15
□ Every 00:30
□ Every 00:45

Scheduled offset: 0 minutes

Random offset: 0 seconds

Server Directory URL :

Transfer Interval Mode :
● All available intervals
○ New intervals since last transfer
○ Fixed number of intervals   Number of intervals 32

Transfer Option : □ Include intervals from previous incomplete transfers

- **PM Transfer Mode**: Configure the operation mode per system. Possible modes are:
  - *Enabled*: Enables PM transfer.
  - *Disabled*: Disables PM transfer.

- **Scheduled Hours**: It is possible to select one or more of the 24 hours in a day, when PM data transfer will happen. Default is none selected.

- **Scheduled Minutes**: It is possible to select one or more of the four 15 minutes in an hour, when PM data transfer will happen. Default is none selected.

- **Scheduled Offset**: It is possible to configure a fixed offset that is added to the scheduled transfer time.

  The range is 0-15 minutes. Default is 0 minute.

  The sum of Scheduled Fixed Offset and Scheduled Random Offset must not exceed 15 minutes.

- **Random Offset**: It is possible to configure a random offset that is added to the scheduled transfer time.

  The offset added to the scheduled transfer time must be a random value in the range 0-Scheduled Offset.

  The range is 0-900 seconds. Default is 0 sec. The sum of Scheduled Offset and Random Offset must not exceed 15 minutes.

- **Server Directory URL**: It is possible to configure the full URL of the server and the corresponding directory (if any) for uploading.

  The supported protocols are HTTP and TFTP.

  To enable HTTP, enter http:// followed by the domain name or IP address.

  To enable TFTP, enter tftp:// followed by the domain name or IP address.

Related Topics

Monitoring Performance Monitor, on page 225

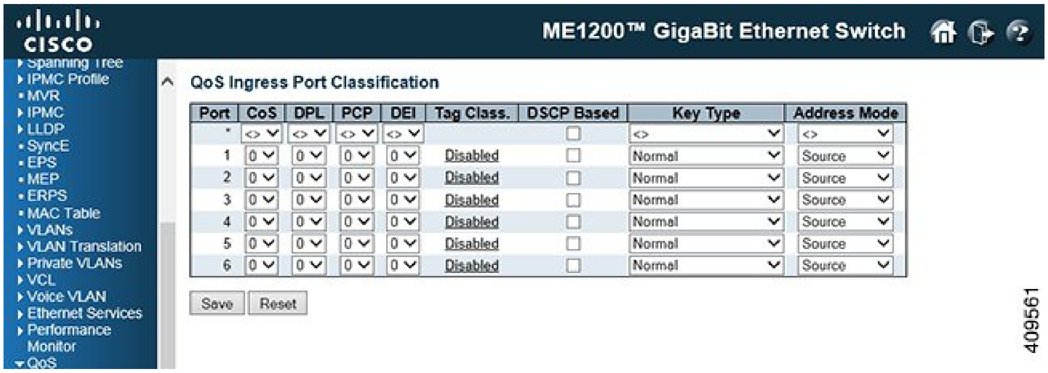
CHAPTER 23

Configuring QoS

The QoS feature available on the ME 1200 Web GUI allows you to do the following:

QoS Ingress Port Classification

This option allows you to configure the basic QoS Ingress Classification settings for all switch ports. The displayed settings are:



QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Key Type	Address Mode
*	<>	<>	<>	<>		□	<>	<>
1	0	0	0	0	Disabled	□	Normal	Source
2	0	0	0	0	Disabled	□	Normal	Source
3	0	0	0	0	Disabled	□	Normal	Source
4	0	0	0	0	Disabled	□	Normal	Source
5	0	0	0	0	Disabled	□	Normal	Source
6	0	0	0	0	Disabled	□	Normal	Source

- **Port**: The port number for which the configuration below applies.
- **CoS**: Controls the default class of service. All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority.

  If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS.The classified CoS can be overruled by a QCL entry.

  Note If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.

- **DPL**: Controls the default drop precedence level. All frames are classified to a drop precedence level.

  If the port is VLAN aware, the frame is tagged and Tag Class. is enabled. Then, the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL.

  The classified DPL can be overruled by a QCL entry.

- **PCP**: Controls the default PCP value. All frames are classified to a PCP value.

  If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.

- **DEI**: Controls the default DEI value. All frames are classified to a DEI value.

  If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.

- **Tag Class**: Shows the classification mode for tagged frames on this port.
  - *Disabled*: Uses default CoS and DPL for tagged frames.
  - *Enabled*: Uses mapped versions of PCP and DEI for tagged frames.

  Click on the mode in order to configure the mode and/or mapping.

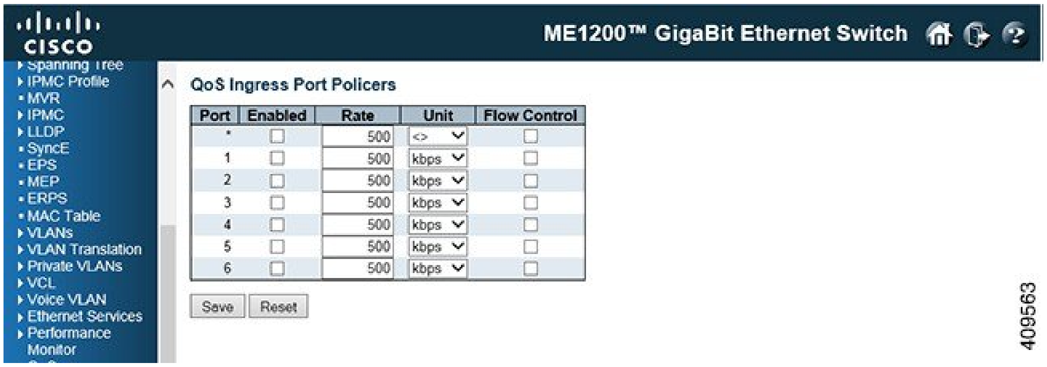
  Note This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.

- **DSCP Based**: Check this check box to enable DSCP Based QoS Ingress Port Classification.
- **Key Type**: The key type specifying the key generated for frames received on the port. The allowed values are:
    - *Normal*: Half key, match outer tag, SIP/DIP and SMAC/DMAC.
    - *Double Tag*: Quarter key, match inner and outer tag.
    - *IP Address*: Half key, match inner and outer tag, SIP and DIP. For non-IP frames, match outer tag only.
    - *MAC and IP Address*: Full key, match inner and outer tag, SMAC, DMAC, SIP and DIP.
    -

    Filtering on DMAC type (unicast/multicast/broadcast) is supported for any key type.
- **Address Mode**: The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. This parameter is only used when the key type is Normal. The allowed values are:
    - *Source*: Enables SMAC/SIP matching.
    - *Destination*: Enables DMAC/DIP matching.

QoS Ingress Port Policer Configuration

This option allows you to configure the Policer settings for all switch ports. The displayed settings are:



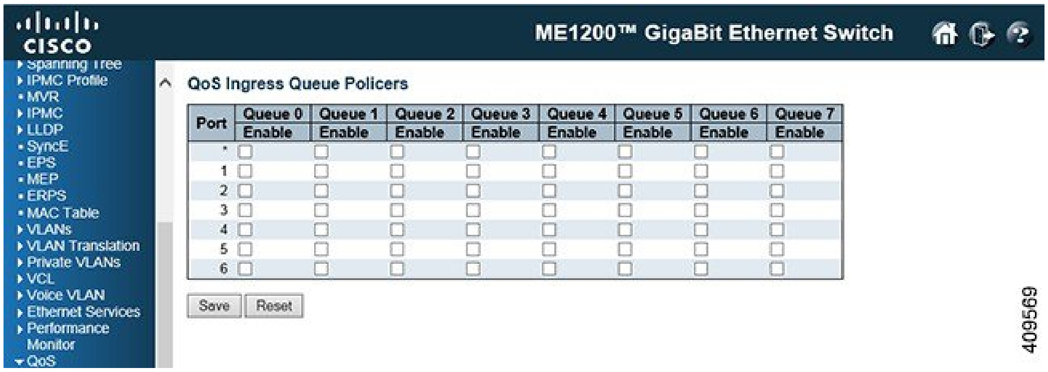
QoS Ingress Port Policers

Port	Enabled	Rate	Unit	Flow Control
*	□	500	<>	□
1	□	500	kbps	□
2	□	500	kbps	□
3	□	500	kbps	□
4	□	500	kbps	□
5	□	500	kbps	□
6	□	500	kbps	□

- **Port**: The port number for which the configuration below applies.
- **Enabled**: Controls whether the policer is enabled on this switch port.
- **Rate**: Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the **Unit** is **kbps** or **fps**, and it is restricted to 1-3300 when the **Unit** is **Mbps** or **kfps**.
- **Unit**: Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps. The default value is **kbps**.
- **Flow Control**: If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

QoS Ingress Queue Policer Configuration

This option allows you to configure the Queue Policer settings for all switch ports. The displayed settings are:



QoS Ingress Queue Policers

Port	Queue 0 Enable	Queue 1 Enable	Queue 2 Enable	Queue 3 Enable	Queue 4 Enable	Queue 5 Enable	Queue 6 Enable	Queue 7 Enable
*	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐

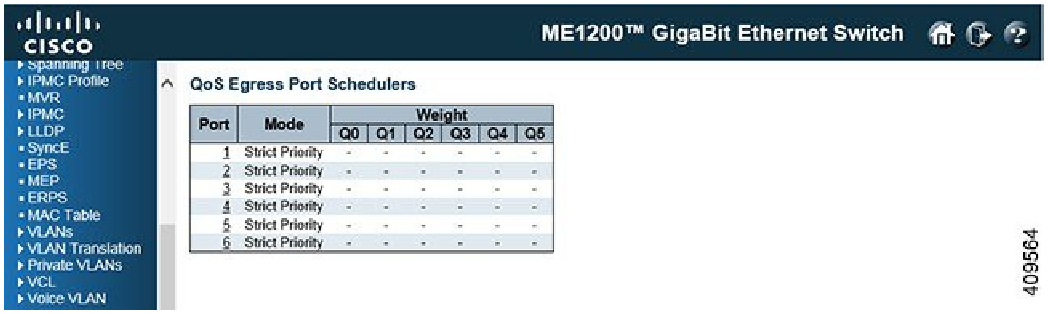
- **Port**: The port number for which the configuration below applies.
- **Enable (E)**: Controls whether the queue policer is enabled on this switch port.
- **Rate**: Controls the rate for the queue policer. The default value is 500. This value is restricted to 100-1000000 when the **Unit** is **kbps**, and it is restricted to 1-3300 when the **Unit** is **Mbps**.

  This field is only shown if at least one of the queue policers is enabled.
- **Unit**: Controls the unit of measure for the queue policer rate as kbps or Mbps. The default value is **kbps**.

  This field is only shown if at least one of the queue policers is enabled.

QoS Egress Port Schedulers

This option provides an overview of QoS Egress Port Schedulers for all switch ports. The displayed settings are:



QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-

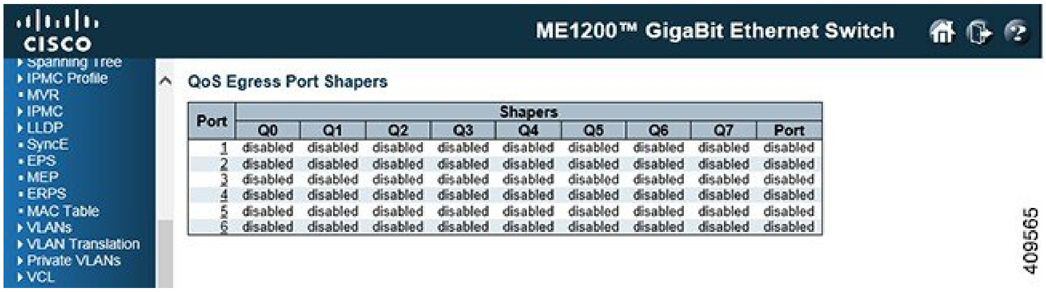
- **Port**: The logical port for the settings contained in the same row.

  Click the port number to configure the schedulers.

- **Mode**: Shows the scheduling mode for this port.
- **Qn**: Shows the weight for this queue and port.

QoS Egress Port Shapers

This option provides an overview of QoS Egress Port Shapers for all switch ports.



QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

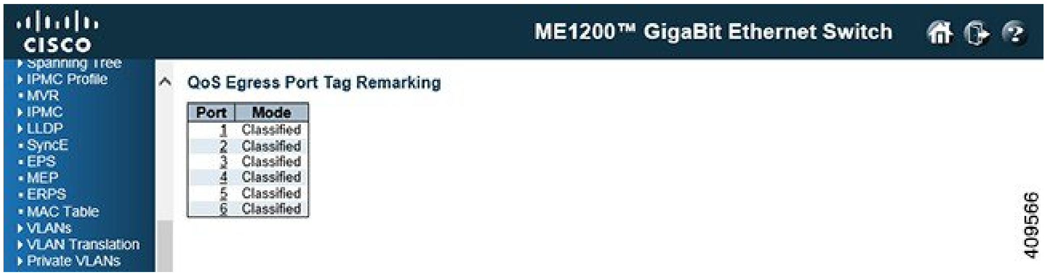
The displayed settings are:

- **Port**: The logical port for the settings contained in the same row.

  Click the port number to configure the shapers.
- **Qn**: Shows *disabled* or actual queue shaper rate, for example 800 Mbps.
- **Port**: Shows *disabled* or actual port shaper rate, for example 800 Mbps.

QoS Egress Port Tag Remarking

This option provides an overview of QoS Egress Port Tag Remarking for all switch ports. The displayed settings are:



QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified

- **Port**: The logical port for the settings contained in the same row.

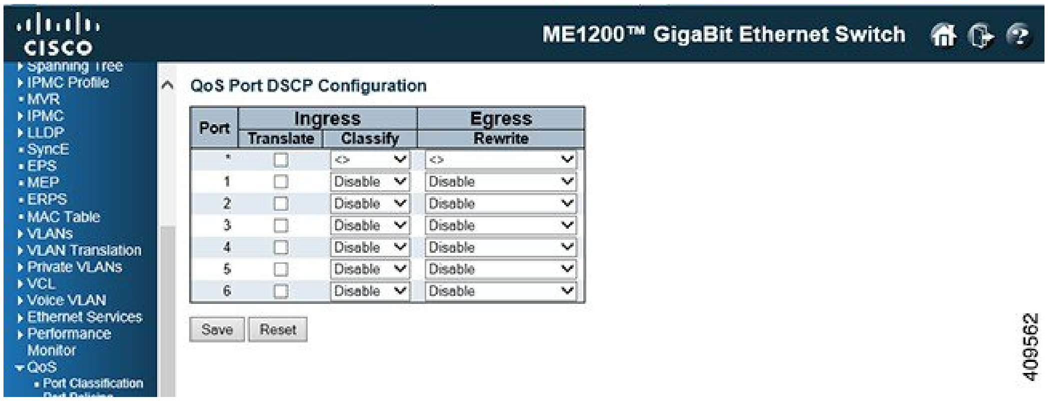
  Click the port number to configure tag remarking.
- **Mode**: Shows the tag remarking mode for this port.
  - *Classified*: Use classified PCP/DEI values.

◦ *Default*: Use default PCP/DEI values.

◦ *Mapped*: Use mapped versions of QoS class and DP level.

Port DSCP Configuration

This option allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports. The displayed settings are:



QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	□	<>	<>
1	□	Disable	Disable
2	□	Disable	Disable
3	□	Disable	Disable
4	□	Disable	Disable
5	□	Disable	Disable
6	□	Disable	Disable

- **Port**: The Port column shows the list of ports for which you can configure dscp ingress and egress settings.
- **Ingress**: In Ingress settings, you can change Ingress translation and classification settings for individual ports.

  There are two configuration parameters available in Ingress:

  - **Translate**: To enable the Ingress Translation, check this check box.
  - **Classify**: Classification for a port has four different values.
    - *Disable*: No Ingress DSCP Classification.
    - *DSCP=0*: Classify if incoming (or translated if enabled) DSCP is 0.
    - *Selected*: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.
    - *All*: Classify all DSCP.

- **Egress**: Port Egress rewriting can have one of the following values:

  ◦ *Disable*: No Egress rewrite.

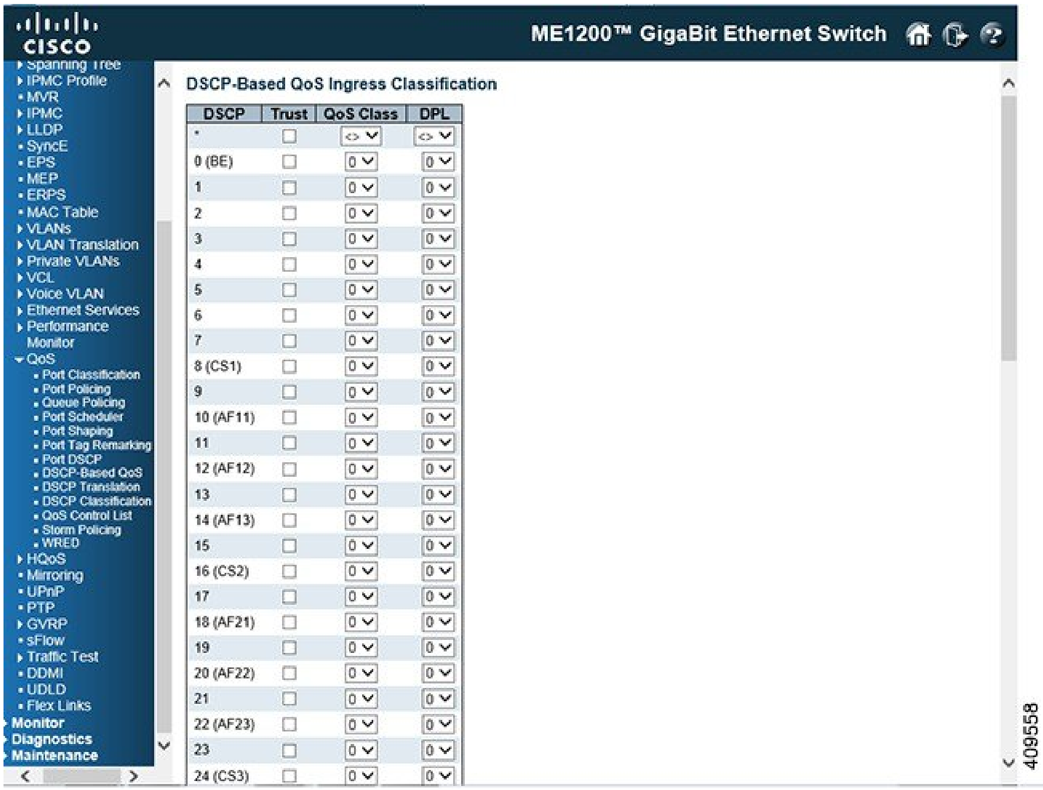
  ◦ *Enable*: Rewrite enabled without remapping.

  ◦ *Remap DP Unaware*: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the**DSCP Translation** > **Egress Remap DP0** table.

◦ *Remap DP Aware*: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the **DSCP Translation** > **Egress Remap DP0** table or from the **DSCP Translation** > **Egress Remap DP1** table.

DSCP-based QoS Ingress Classification

This option allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.



DSCP-Based QoS Ingress Classification

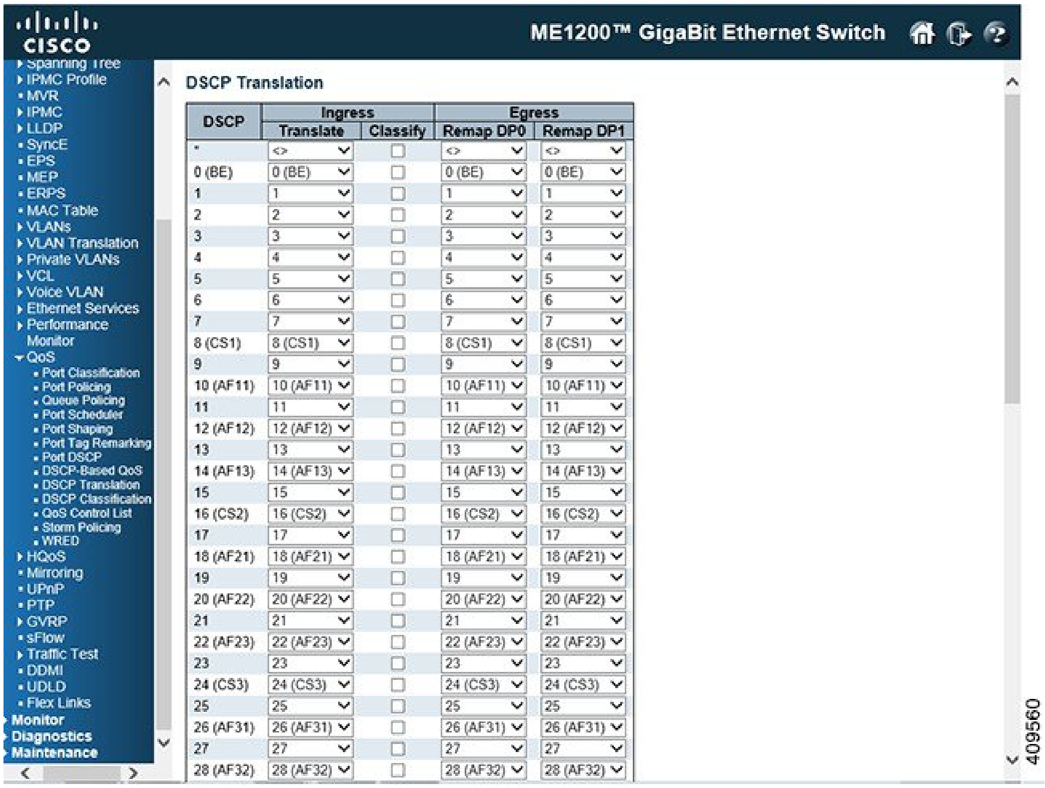
DSCP	Trust	QoS Class	DPL
*	□	<>	<>
0 (BE)	□	0	0
1	□	0	0
2	□	0	0
3	□	0	0
4	□	0	0
5	□	0	0
6	□	0	0
7	□	0	0
8 (CS1)	□	0	0
9	□	0	0
10 (AF11)	□	0	0
11	□	0	0
12 (AF12)	□	0	0
13	□	0	0
14 (AF13)	□	0	0
15	□	0	0
16 (CS2)	□	0	0
17	□	0	0
18 (AF21)	□	0	0
19	□	0	0
20 (AF22)	□	0	0
21	□	0	0
22 (AF23)	□	0	0
23	□	0	0
24 (CS3)	□	0	0

The displayed settings are:

- **DSCP**: Maximum number of supported DSCP values are 64.
- **Trust**: Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.
- **QoS Class**: QoS class can be any value in the range 0-7.
- **DPL**: Drop Precedence Level (0-1).

DSCP Translation

This option allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.



DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	□	<>	<>
0 (BE)	0 (BE)	□	0 (BE)	0 (BE)
1	1	□	1	1
2	2	□	2	2
3	3	□	3	3
4	4	□	4	4
5	5	□	5	5
6	6	□	6	6
7	7	□	7	7
8 (CS1)	8 (CS1)	□	8 (CS1)	8 (CS1)
9	9	□	9	9
10 (AF11)	10 (AF11)	□	10 (AF11)	10 (AF11)
11	11	□	11	11
12 (AF12)	12 (AF12)	□	12 (AF12)	12 (AF12)
13	13	□	13	13
14 (AF13)	14 (AF13)	□	14 (AF13)	14 (AF13)
15	15	□	15	15
16 (CS2)	16 (CS2)	□	16 (CS2)	16 (CS2)
17	17	□	17	17
18 (AF21)	18 (AF21)	□	18 (AF21)	18 (AF21)
19	19	□	19	19
20 (AF22)	20 (AF22)	□	20 (AF22)	20 (AF22)
21	21	□	21	21
22 (AF23)	22 (AF23)	□	22 (AF23)	22 (AF23)
23	23	□	23	23
24 (CS3)	24 (CS3)	□	24 (CS3)	24 (CS3)
25	25	□	25	25
26 (AF31)	26 (AF31)	□	26 (AF31)	26 (AF31)
27	27	□	27	27
28 (AF32)	28 (AF32)	□	28 (AF32)	28 (AF32)

The displayed settings are:

- **DSCP**: Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.
- **Ingress**: Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.

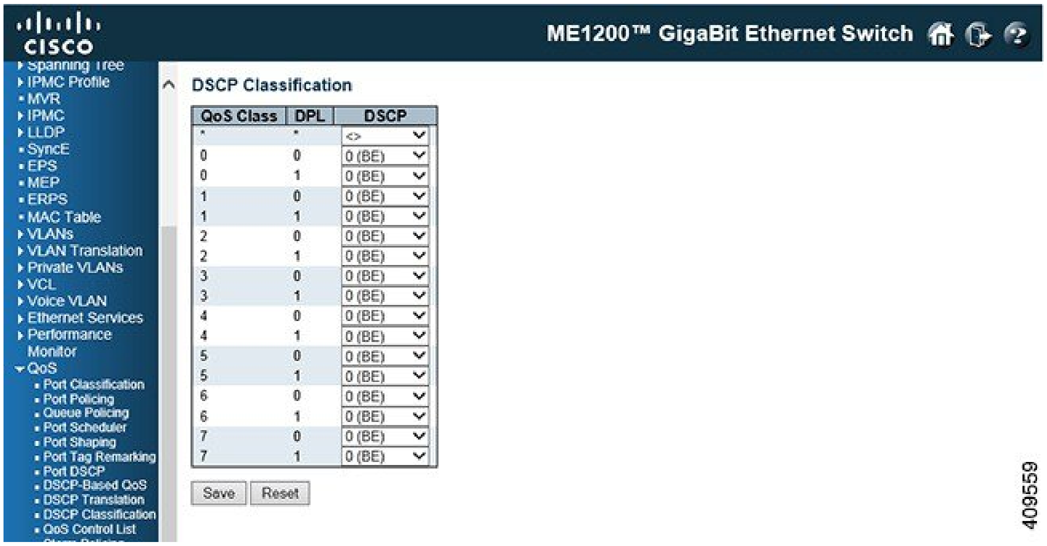
  There are two configuration parameters for DSCP Translation:

  - **Translate**: DSCP at Ingress side can be translated to any of the DSCP values in the range 0-63.
  - **Classify**: Check this check box to enable classification at Ingress side.

- **Egress**: The following parameters are configurable for Egress side:
  - **Remap DP0**: Controls the remapping for frames with DP level 0. Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.
  - **Remap DP1** Controls the remapping for frames with DP level 1. Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

DSCP Classification

This option allows you to configure the mapping of QoS class and Drop Precedence Level to DSCP value. The displayed settings are:



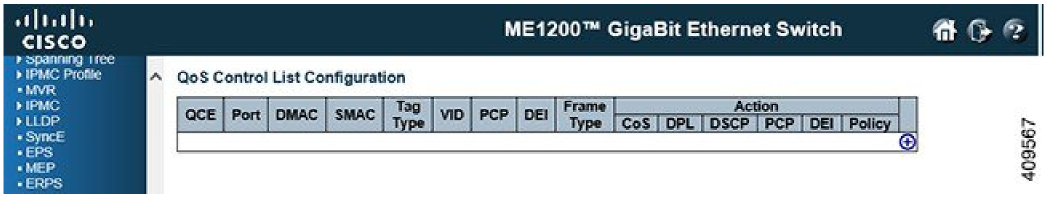
DSCP Classification

QoS Class	DPL	DSCP
*	*	<>
0	0	0 (BE)
0	1	0 (BE)
1	0	0 (BE)
1	1	0 (BE)
2	0	0 (BE)
2	1	0 (BE)
3	0	0 (BE)
3	1	0 (BE)
4	0	0 (BE)
4	1	0 (BE)
5	0	0 (BE)
5	1	0 (BE)
6	0	0 (BE)
6	1	0 (BE)
7	0	0 (BE)
7	1	0 (BE)

- **QoS Class**: Actual QoS class.
- **DPL**: Actual Drop Precedence Level.
- **DSCP**: Select the classified DSCP value (0-63).

QoS Control List Configuration

This option shows the QoS Control List (QCL) which is made up of the QoS Control Entries (QCEs). Each row describes a QCE that is defined. The maximum number of QCEs is 1024 on each switch.



QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action					
									CoS	DPL	DSCP	PCP	DEI	Policy

Click the **Add QCE to end of list** icon to add a new QCE to the list.

- **QCE**: Indicates the QCE ID.
- **Port**: Indicates the list of ports configured with the QCE or Any.
- **DMAC**: Indicates the destination MAC address. Possible values are:

    - *Any*: Match any DMAC.
    - *Unicast*: Match unicast DMAC.
    - *Multicast*: Match multicast DMAC.
    - *Broadcast*: Match broadcast DMAC.
    - *<MAC>*: Match specific DMAC.

  The default value is **Any**.

- **SMAC**: Match specific source MAC address or **Any**. If a port is configured to match on destination addresses, this field indicates the DMAC.
- **Tag Type**: Indicates tag type. Possible values are:
    - *Any*: Match tagged and untagged frames.
    - *Untagged*: Match untagged frames.
    - *Tagged*: Match tagged frames.
    - *C-Tagged*: Match C-tagged frames.
    - *S-Tagged*: Match S-tagged frames.

  The default value is **Any**.

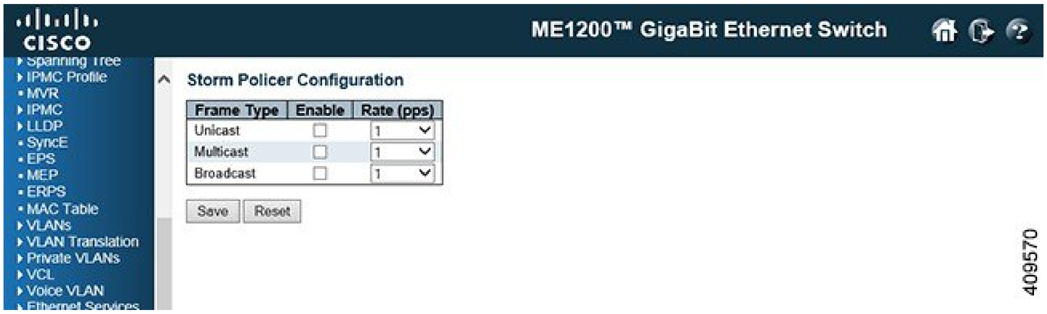
- **VID**: Indicates VLAN ID, either a specific VID or range of VIDs. VID can be in the range 1-4095 or **Any**.
- **PCP**: Priority Code Point: Valid values of PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or **Any**.
- Drop Eligible Indicator (**DEI**): Valid value of DEI are 0, 1 or **Any**.
- **Frame Type**: Indicates the type of frame. Possible values are:
    - *Any*: Match any frame type.
    - *Ethernet*: Match EtherType frames.
    - *LLC*: Match (LLC) frames.
    - *SNAP*: Match (SNAP) frames.
    - *IPv4*: Match IPv4 frames.
    - *IPv6*: Match IPv6 frames.
- **Action**: Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are:
    - **CoS**: Classify Class of Service.
    - **DPL**: Classify Drop Precedence Level.
    - **DSCP**: Classify DSCP value.
    - **PCP**: Classify PCP value.
    - **DEI**: Classify DEI value.

  - **Policy**: Classify ACL Policy number.

- Modification icons: You can modify each QCE in the table using the following buttons:
  - **Insert QCE before this QCE** icon: Inserts a new QCE before the current row.
  - **Edit QCE** icon: Edits the QCE.
  - **Move QCE up** icon: Moves the QCE up the list.
  - **Move QCE down** icon: Moves the QCE down the list.
  - **Delete QCE** icon: Deletes the QCE.
  - **Add QCE to end of list** icon: The lowest plus sign adds a new entry at the bottom of the QCE listings.

Storm Policer Configuration

This option allows you to configure the Storm policers for the switch.



Storm Policer Configuration

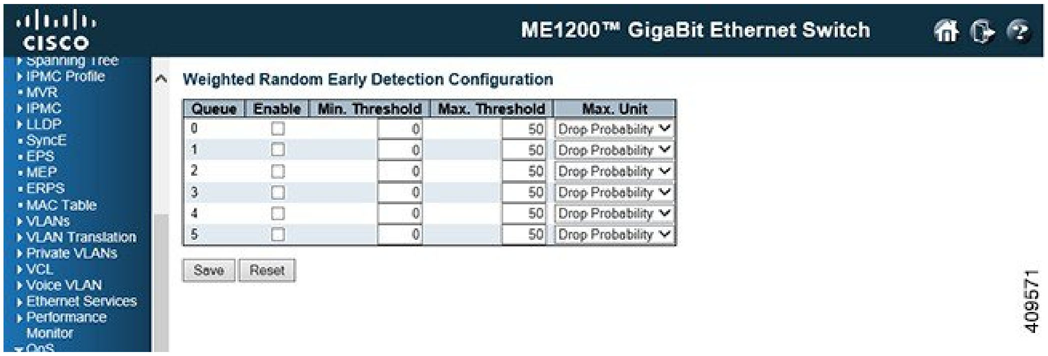
Frame Type	Enable	Rate (pps)
Unicast	□	1
Multicast	□	1
Broadcast	□	1

There is a unicast storm policer, multicast storm policer, and a broadcast storm policer. These only affect flooded frames, that is, frames with a (VLAN ID, DMAC) pair not present on the MAC address table. The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch.

- **Frame Type**: The settings in a particular row apply to the frame type listed here: Unicast, Multicast or Broadcast.
- **Enable**: Enable or disable the storm policer for the given frame type.
- **Rate**: The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K.

QoS Weighted Random Early Detection

This option allows you to configure the Random Early Detection (RED) settings for queue 0 to 5.



Weighted Random Early Detection Configuration

Queue	Enable	Min. Threshold	Max. Threshold	Max. Unit
0	□	0	50	Drop Probability
1	□	0	50	Drop Probability
2	□	0	50	Drop Probability
3	□	0	50	Drop Probability
4	□	0	50	Drop Probability
5	□	0	50	Drop Probability

RED cannot be applied to queue 6 and 7.

Through different RED configuration for the queues (QoS classes), it is possible to obtain Weighted Random Early Detection (WRED) operation between queues.

The settings are global for all ports in the switch.The displayed settings are:

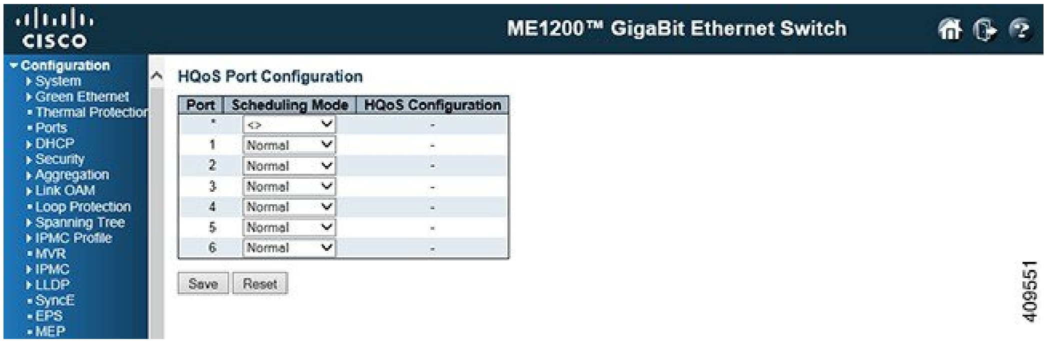
- **Queue**: The queue number (QoS class) for which the configuration below applies.
- **Enable**: Controls whether RED is enabled for this queue.
- **Min. Threshold**: Controls the lower RED fill level threshold. If the queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100%.
- **Max. Threshold**: Controls the upper RED drop probability or fill level threshold for frames marked with Drop Precedence Level 1 (yellow frames). This value is restricted to 1-100% Max.
- **Max. Unit**: Selects the unit for **Max. Threshold**. Possible values are:
  - *Drop Probability*: **Max. Threshold** controls the drop probability just below 100% fill level.
  - *Fill Level*: **Max. Threshold** controls the fill level where drop probability reaches 100%.

CHAPTER 24

Configuring HQoS

The HQoS feature available on the ME 1200 Web GUI allows you to configure the HQoS port and HQoS entries.

HQoS Port Configuration



HQoS Port Configuration

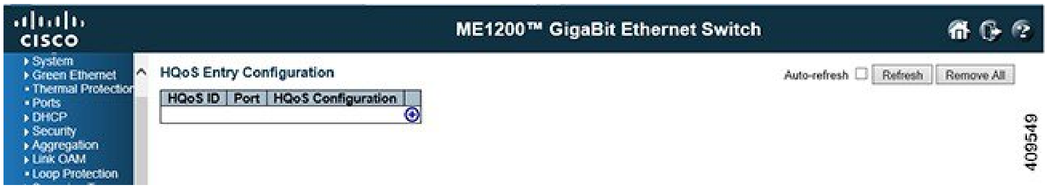
Port	Scheduling Mode	HQoS Configuration
*	<>	-
1	Normal	-
2	Normal	-
3	Normal	-
4	Normal	-
5	Normal	-
6	Normal	-

This option displays current HQoS port configurations. The settings can also be configured here.

- **Port**: The logical port for the settings contained in the same row.
- **Scheduling Mode**: The scheduling mode for the port affects which egress QoS options are available. The allowed values are:
  - *Normal*: Normal QoS configuration available for non-service traffic only.
  - *Basic*: Basic QoS configuration available for non-service traffic only.
  - *Hierarchical*: Basic QoS configuration available per HQoS entry.
- **HQoS Configuration**: Link to Hierarchical Quality of Service configuration for ports in Hierarchical Scheduling Mode.

HQoS Entry Configuration

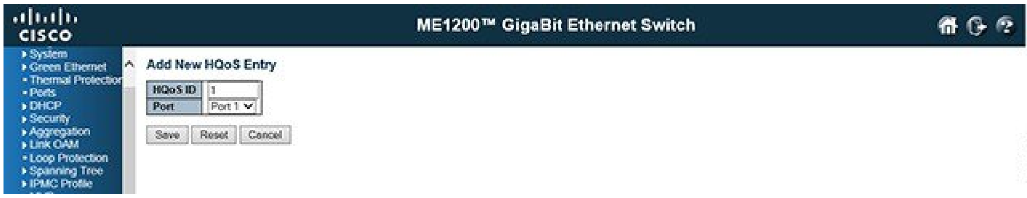
This option displays currently configured HQoS entries.



HQoS Entry Configuration

HQoS ID	Port	HQoS Configuration

- **HQoS ID**: The HQoS ID identifies the HQoS entry. The range is from 1 through 256.
- **Port**: The destination port for the traffic mapped to the HQoS entry.
- **HQoS Configuration**: Displays a link to the QoS parameter configuration.
- Modification icons: You can add or delete HQoS entries in the table using the following icons:
  - **Delete HQoS Entry** icon: Deletes the HQoS entry.
  - **Add New HQoS Entry** icon: Adds new HQoS entry as shown in the following figure.



Add New HQoS Entry

HQoS ID	1
Port	Port 1

CHAPTER 25

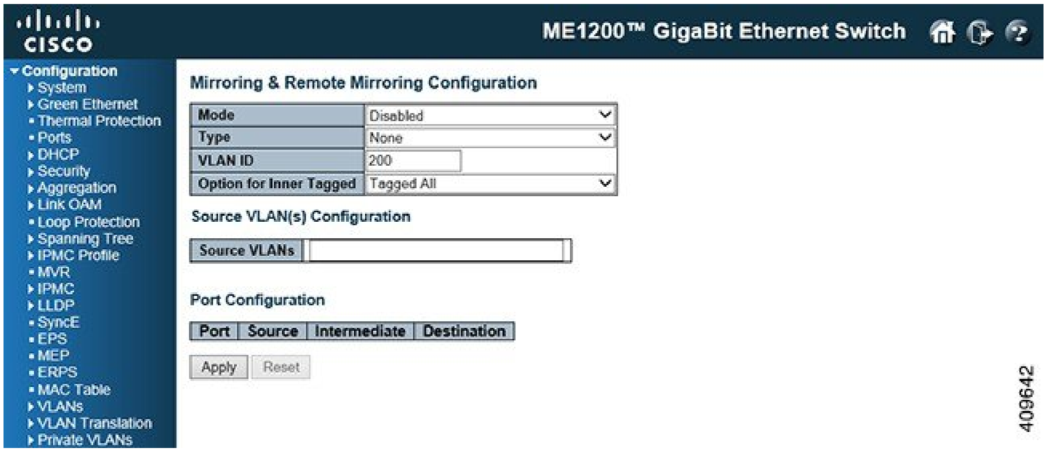
Configuring Mirroring

Mirroring and Remote Mirroring Configuration

Mirroring is a feature for switched port analyzer. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.

Remote Mirroring is an extend function of Mirroring. It can extend the destination port in other switch. So the administrator can analyze the network traffic on the other switches.

If a frame is mirrored by more than one mirror probe, then the highest numbered probe is selected. This implies that only one mirror copy is made per frame even if multiple probes are active.



Mirroring & Remote Mirroring Configuration

Mode	Disabled
Type	None
VLAN ID	200
Option for Inner Tagged	Tagged All

Source VLAN(s) Configuration

Source VLANs	

Port Configuration

Port	Source	Intermediate	Destination

- **Mode**: Enables or disables the mirror or Remote Mirroring function.
- **Type**: Selects switch type.
  - *Mirror*: The switch is running on mirror mode. The source port(s) and destination port are located on this switch.

- *Source*: The switch is a source node for monitor flow. The source port(s) and intermediate port(s) are located on this switch.
- *Intermediate*: The switch is a forwarding node for monitor flow and the switch is an option node. The object is to forward traffic from source switch to destination switch. The intermediate ports are located on this switch.
- *Destination*: The switch is an end node for monitor flow. The destination port(s) and intermediate port(s) are located on this switch.

- **VLAN ID**: The VLAN ID points out where the monitor packet will copy to. The default VLAN ID is 200.
- **Option for Inner Tagged**: Select an inner tagged or an inner untagged type.

Source VLAN(s) Configuration: The switch can supports VLAN-based Mirroring. If you want to monitor some VLANs on the switch, you can set the selected VLANs on this field.

Note The Mirroring session shall have either ports or VLANs as sources, but not both.

Port Configuration: The following options are used for port role selecting:

- **Port**: The logical port for the settings contained in the same row. The CPU also can be selected
- **Source**: Selects mirror mode.
  - *Disabled*: Neither frames transmitted nor frames received are mirrored.
  - *Both*: Frames received and frames transmitted are mirrored on the Intermediate/Destination port.
  - *Rx only*: Frames received on this port are mirrored on the Intermediate/Destination port. Frames transmitted are not mirrored.
  - *Tx only*: Frames transmitted on this port are mirrored on the Intermediate/Destination port. Frames received are not mirrored.
- **Intermediate**: Select intermediate port. This checkbox is designed for Remote Mirroring. The intermediate port is a switched port to connect to other switch. All packets that are going through intermediate port will be tagged when the rmirror function is enabled.

  Note The intermediate port needs to disable MAC Table learning.

- **Destination**: Select destination port. This checkbox is designed for mirror or Remote Mirroring. The destination port is a switched port that you receive a copy of traffic from the source port.

  Note On mirror mode, the device only supports one destination port.

  Note The destination port needs to disable MAC Table learning.

Configuration Guideline for All Features

When the switch is running on Remote Mirroring mode, the administrator also needs to check whether or not other features are enabled or disabled. All recommended settings are described as follows.

Feature	Impact	source port	intermediate port	destination port	Remote Mirroring VLAN
arp_inspection	High		* disabled		
acl	Critical		* disabled	* disabled	
dhcp_relay	High		* disabled		
dhcp_snooping	High	* disabled			
ip_source_guard	Critical	* disabled	* disabled		
ipmc/igmpsnp	Critical				un-conflict
ipmc/mldsnp	Critical				un-conflict
lacp	Low			o disabled	
lldp	Low			o disabled	
mac learning	Critical		* disabled	* disabled	
mstp	Critical			o disabled	
mvr	Critical				un-conflict
nas	Critical		* authorized	* authorized	
psec	Critical		* disabled	* disabled	
qos	Critical		* unlimited	* unlimited	
upnp	Low			o disabled	
mac-based vlan	Critical		* disabled		
protocol-based vlan	Critical		* disabled		
vlan_translation	Critical		* disabled	* disabled	
voice_vlan	Critical		* disabled		
mrp	Low		o disabled		
mvrp	Low		o disabled		

Note

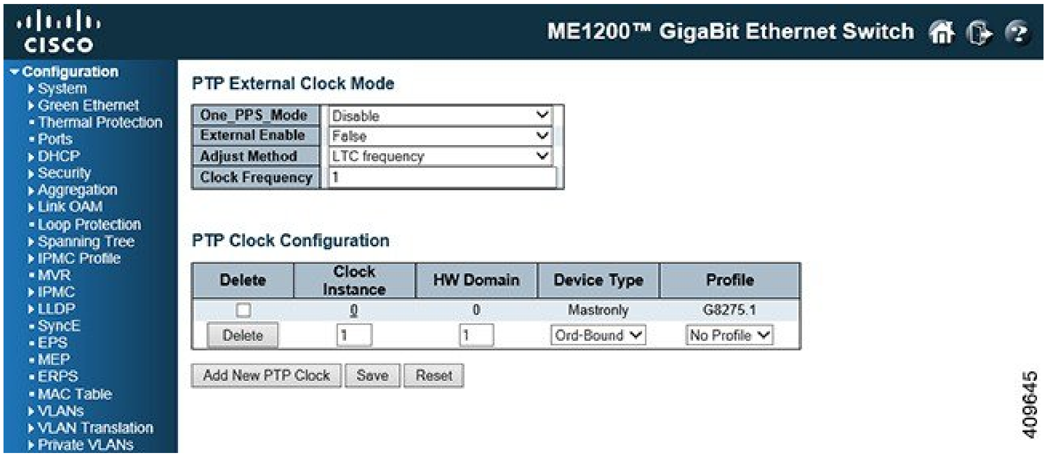
- * -- must
- o -- optional
- Impact: Critical/High/Low
- Critical 5 packets -> 0 packet
- High 5 packets -> 4 packets
- Low 5 packets -> 6 packets

CHAPTER 26

Configuring PTP

PTP Clock Configuration

This feature allows you to configure and inspect the current PTP clock settings.



PTP External Clock Mode

One_PPS_Mode	Disable
External Enable	False
Adjust Method	LTC frequency
Clock Frequency	1

PTP Clock Configuration

Delete	Clock Instance	HW Domain	Device Type	Profile
□	0	0	Mastronly	G8275.1
Delete	1	1	Ord-Bound	No Profile

PTP External Clock Mode

- **One_PPS_Mode**: This drop-down list allows you to select the One_pps_mode configuration. The following values are possible:
    - *Output*: Enables the 1 pps clock output.
    - *Input*: Enables the 1 pps clock input.
    - *Disable*: Disables the 1 pps clock input or output.
- **External Enable**: This drop-down list allows you to configure the external cock output. The following values are possible:
    - *True*: Enables the external clock output.

  - *False*: Disables the external clock output.

- **Adjust Method**: This drop-down list allows you to configure the frequency adjustment configuration.
  - *LTC frequency*: Selects Local Time Counter (LTC) frequency control.
  - *SyncE-DPLL*: Selects SyncE DPLL frequency control, if allowed by SyncE.
  - *Oscillator*: Selects an oscillator independent of SyncE for frequency control, if supported by the hardware.
  - *LTC phase*: Selects Local Time Counter (LTC) phase control (assumes that the frequency is locked by means of SyncE).

- **Clock Frequency**: This will allow to set the Clock Frequency.The possible range of values are 1 - 25000000 (1 - 25MHz).

PTP Clock Configuration

- **Delete**: Check the corresponding check box and click **Save** to delete a clock instance.
- **Clock Instance**: Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to edit the Clock details.
- **HW Domain**: Indicates the HW clock domain used by the clock.
- **Device Type**: Indicates the Type of the Clock Instance. There are five Device Types.
  - *Ord-Bound* - clock's Device Type is Ordinary-Boundary Clock.
  - *P2p Transp* - clock's Device Type is Peer to Peer Transparent Clock.
  - *E2e Transp* - clock's Device Type is End to End Transparent Clock.
  - *Master Only* - clock's Device Type is Master Only.
  - *Slave Only* - clock's Device Type is Slave Only.

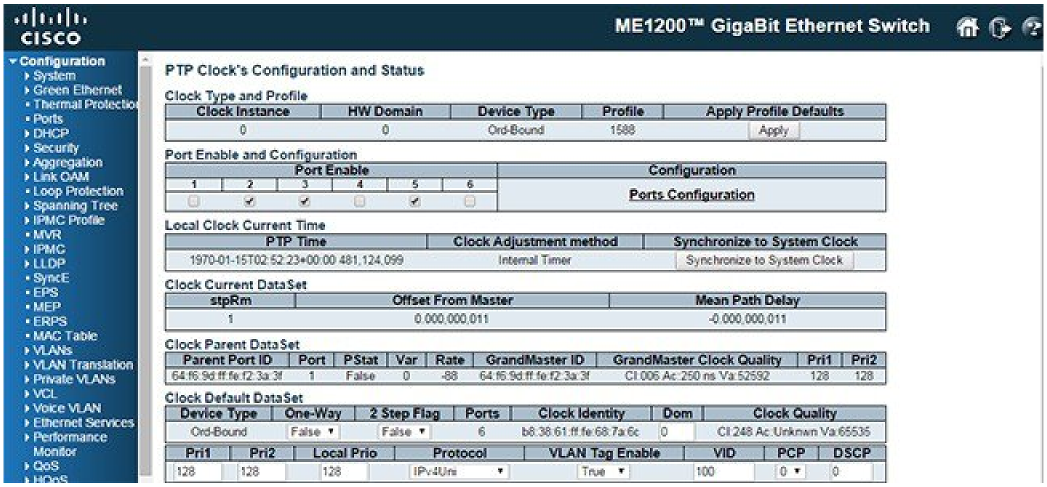
- **Profile**: Indicates the profile used by the clock. The different PTP profiles available are as follows:
  - G8275.1
  - G8265.1
  - IEEE1588

Related Topics

Monitoring PTP, on page 231

PTP Clock's Configuration for an Instance

This option allows you to inspect and configure the current PTP clock settings.



PTP Clock's Configuration and Status

Clock Type and Profile

Clock Instance	HW Domain	Device Type	Profile	Apply Profile Defaults
0	0	Ord-Bound	1588	Apply

Port Enable and Configuration

Port Enable						Configuration
1	2	3	4	5	6	
□	☑	☑	□	☑	□	Ports Configuration

Local Clock Current Time

PTP Time	Clock Adjustment method	Synchronize to System Clock
1970-01-15T02:52:23+00:00 481,124,099	Internal Timer	Synchronize to System Clock

Clock Current DataSet

stpRm	Offset From Master	Mean Path Delay
1	0.000,000,011	-0.000,000,011

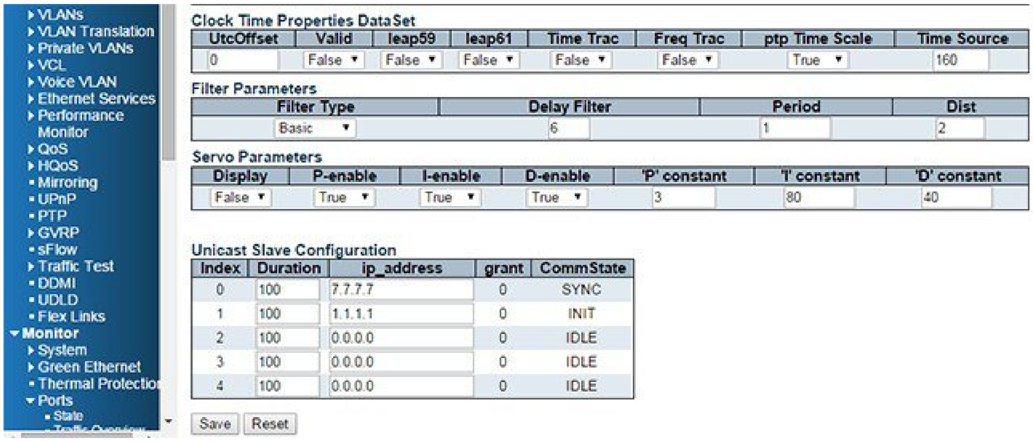
Clock Parent DataSet

Parent Port ID	Port	PStat	Var	Rate	GrandMaster ID	GrandMaster Clock Quality	Pri1	Pri2
64:f6:9d:ff:fe:f2:3a:3f	1	False	0	-88	64:f6:9d:ff:fe:f2:3a:3f	Cl:006 Ac:250 ns Va:52592	128	128

Clock Default DataSet

Device Type	One-Way	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality
Ord-Bound	False	False	6	b8:38:61:ff:fe:68:7a:6c	0	Cl:248 Ac:Unknwn Va:65535

Pri1	Pri2	Local Prio	Protocol	VLAN Tag Enable	VID	PCP	DSCP
128	128	128	IPv4Uni	True	100	0	0



Clock Time Properties DataSet

UtcOffset	Valid	leap59	leap61	Time Trac	Freq Trac	ptp Time Scale	Time Source
0	False	False	False	False	False	True	160

Filter Parameters

Filter Type	Delay Filter	Period	Dist
Basic	6	1	2

Servo Parameters

Display	P-enable	I-enable	D-enable	'P' constant	'I' constant	'D' constant
False	True	True	True	3	80	40

Unicast Slave Configuration

Index	Duration	ip_address	grant	CommState
0	100	7.7.7.7	0	SYNC
1	100	1.1.1.1	0	INIT
2	100	0.0.0.0	0	IDLE
3	100	0.0.0.0	0	IDLE
4	100	0.0.0.0	0	IDLE

Save Reset

Clock Type and Profile

- **Clock Instance**: Indicates the instance number of a particular Clock Instance [0..3].
- **HW Domain**: Indicates the HW clock domain used by the clock.
- **Device Type**: Indicates the Type of the Clock Instance. There are five Device Types.
  - *Ord-Bound* - clock's Device Type is Ordinary-Boundary Clock.
  - *P2p Transp* - clock's Device Type is Peer to Peer Transparent Clock.
  - *E2e Transp* - clock's Device Type is End to End Transparent Clock.
  - *Master Only* - clock's Device Type is Master Only.
  - *Slave Only* - clock's Device Type is Slave Only.
- **Profile**: Indicates the profile used by the clock.
- **Apply Profile Defaults**: If the clock has been configured to use a profile, clicking the **Apply** button will reset configured values to profile defaults.

Port Enable and Configuration

- **Port Enable**: Check the corresponding check box for each port configured for this Clock Instance.
- **Configuration**: Click **Ports Configuration** to edit the port data set for the ports assigned to this clock instance.

Local Clock Current Time: Show or update local clock data.

- **PTP Time**: Shows the actual PTP time with nanosecond resolution.
- **Clock Adjustment method**: Shows the actual clock adjustment method. The method depends on the available hardware.
- **Synchronize to System Clock**: Activate this button to synchronize the System Clock to PTP Time.

Clock Current DataSet: The clock current data set is defined in the IEEE 1588 Standard. The current data set is dynamic.

- Steps Removed (**stpRm**): It is the number of PTP clocks traversed from the grandmaster to the local slave clock.
- **Offset From Master**: Time difference between the master clock and the local slave clock, measured in ns.
- **Mean Path Delay**: The mean propagation time for the link between the master and the local slave.

Clock Parent DataSet: The clock parent data set is defined in the IEEE 1588 standard. The parent data set is dynamic.

- **Parent Port ID**: Clock identity for the parent clock. If the local clock is not a slave, the value is the clock's own id.
- **Port**: Port Id for the parent master port.
- **PStat**: Parent's Stats (always **False**).
- **Var**: It is observed parent offset scaled log variance.
- **Rate**: Observed Parent Clock Phase Change Rate that is, the slave clocks rate offset compared to the master. (unit = ns per s).
- **GrandMaster ID**: Clock identity for the grand master clock. If the local clock is not a slave, the value is the clock's own id.
- **GrandMaster Clock Quality**: The clock quality announced by the grand master (See the description of Clock Default DataSet: Clock Quality).
- **Pri1**: Clock priority 1 announced by the grand master.
- **Pri2**: Clock priority 2 announced by the grand master.

Clock Default DataSet: The clock default data set is defined in the IEEE 1588 Standard. It holds three groups of data: the static members defined at clock creation time, the Dynamic members defined by the system, and the configurable members which can be set here.

- **Device Type**: Indicates the Type of the Clock Instance. There are five Device Types.
    - *Ord-Bound* - clock's Device Type is Ordinary-Boundary Clock.

  - *P2p Transp* - clock's Device Type is Peer to Peer Transparent Clock.
  - *E2e Transp* - clock's Device Type is End to End Transparent Clock.
  - *Master Only* - clock's Device Type is Master Only.
  - *Slave Only* - clock's Device Type is Slave Only.

- **2 Step Flag**: *True* if two-step Sync events and Pdelay_Resp events are used.
- **One-Way**: If *True*, one way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, that is, this is applicable only if frequency synchronization is needed. The master always responds to delay requests.
- **Ports**: The total number of physical ports in the node.
- **Clock Identity**: It shows unique clock identifier.
- **Dom**: Clock domain [0..127].
- **Clock Quality**: The clock quality is determined by the system, and holds three parts: Clock Class, Clock Accuracy and OffsetScaledLog Variance as defined in IEEE1588.The Clock Accuracy values are defined in IEEE1588 table 6 (Currently, the clock Accuracy is set to 'Unknown' as default).
- **Pri1**: Clock priority 1 [0..255] used by the BMC master select algorithm
- **Pri2**: Clock priority 2 [0..255] used by the BMC master select algorithm.
- **Protocol**: Transport protocol used by the PTP protocol engine. The following values are possible:
  - *Ethernet*: PTP over Ethernet multicast.
  - *EthernetMixed*: PTP using a combination of Ethernet multicast and unicast.
  - *Pv4Multi*: PTP over IPv4multicast.
  - *IPv4Mixed*: PTP using a combination of IPv4 multicast and unicast.
  - *IPv4Uni*: PTP over IPv4 unicast.
- **VLAN Tag Enable**: The VLAN Tag Enable parameter is ignored, because the tagging is controlled by the VLAN configuration.
- **VID**: VLAN Identifier used for tagging the VLAN packets.
- **PCP**: Priority Code Point value used for PTP frames.

Clock Time Properties DataSet: The clock time properties data set is defined in the IEEE 1588 Standard. The data set is both configurable and dynamic, that is, the parameters can be configured for a grandmaster. In a slave clock the parameters are overwritten by the grandmaster's timing properties. The parameters are not used in the current PTP implementation. The valid values for the **Time Source** parameter are:

- 16 (0x10) ATOMIC_CLOCK
- 32 (0x20) GPS
- 48 (0x30) TERRESTRIAL_RADIO
- 64 (0x40) PTP
- 80 (0x50) NTP

- 96 (0x60) HAND_SET
- 144 (0x90) OTHER
- 160 (0xA0) INTERNAL_OSCILLATOR

Filter Parameters: The default delay filter is a low pass filter, with a time constant of 2****Delay Filter***DelayRequestRate.

If the **Delay Filter** parameter is set to 0 or the **Dist** parameter is 0, the delay filter uses the same algorithm as the offset filter. The default offset filter uses a minimum offset or a mean filter method that is, the minimum measured offset during **Period** samples is used in the calculation. The distance between two calculations is Dist periods.

Note In configurations with Timestamp enabled PHYs, the period is automatically increased, if period*dist < SyncPackets per sec/4, that is, max four adjustments are made per sec.

- **Filter Type**: Shows the filter type used which can be either the basic filter or an advanced filter that can be configured to use only a fraction of the packets received (that is, the packets that have experienced the least latency).
- **Delay Filter**: See above.
- **Period**: See above.
- **Dist**: See above.

Servo Parameters: The default clock servo uses a PID regulator to calculate the current clock rate that is,

clockAdjustment =

OffsetFromMaster/ P constant +

Integral(OffsetFromMaster)/ I constant +

Differential OffsetFromMaster)/ D constant

- **Display**: If *True*, then Offset From Master, MeanPathDelay and clockAdjustment are logged on the debug terminal.
- **P-enable**: If *True*, the P part of the algorithm is included.
- **I-enable**: If *True*, the I part of the algorithm is included.
- **D-enable**: If *True*, the D part of the algorithm is included.
- **'P' constant**: [1..1000] See above.
- **'I' constant**: [1..1000] See above.
- **'D' constant**: [1..1000] See above.

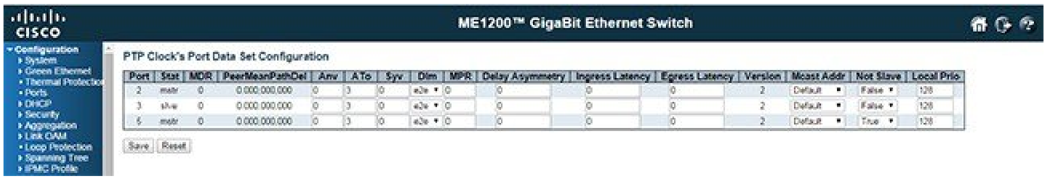
Unicast Slave Configuration: When operating in IPv4 Unicast mode, the slave is configured up to five master IP addresses. The slave then requests Announce messages from all the configured masters. The slave uses the BMC algorithm to select one as master clock, the slave then request Sync messages from the selected master.

- **Duration**: The number of seconds a master is requested to send Announce/Sync messages. The request is repeated from the slave each Duration/4 seconds.

- **ip_address**: IPv4 Address of the Master clock.
- **grant**: The granted repetition period for the sync message.
- **CommState**: The state of the communication with the master, possible values are:
    - *IDLE*: The entry is not in use.
    - *INIT*: Announce is sent to the master (Waiting for a response).
    - *CONN*: The master has responded.
    - *SELL*: The assigned master is selected as current master.
    - *SYNC*: The master is sending Sync messages.

PTP Clock's Port Configuration

The port data set is defined in the IEEE 1588 Standard. It holds three groups of data: the static members, the dynamic members, and configurable members which can be set here.



PTP Clock's Port Data Set Configuration

Port	Stat	MDR	PeerMeanPathDel	Anv	ATo	Syv	Dlm	MPR	Delay Asymmetry	Ingress Latency	Egress Latency	Version	Mcast Addr	Not Slave	Local Prio
2	mstr	0	0.000,000,000	0	3	0	e2e	0	0	0	0	2	Default	False	128
3	slve	0	0.000,000,000	0	3	0	e2e	0	0	0	0	2	Default	False	128
5	mstr	0	0.000,000,000	0	3	0	e2e	0	0	0	0	2	Default	True	128

Port Data Set

- **Port**: Static member port Identity. Port number [1..max port no].
- **Stat**: Dynamic member port State. Current state of the port.
- **MDR**: Dynamic member log Min Delay Req Interval. The delay request interval announced by the master.
- **PeerMeanPathDel**: The path delay measured by the port in P2P mode. In E2E mode this value is 0.
- **Anv**: The interval for issuing announce messages in master state. Range is -3 to 4.
- **ATo**: The timeout for receiving announce messages on the port. Range is 1 to 10.
- **Syv**: The interval for issuing sync messages in master. Range is -7 to 4.
- Configurable member delay mechanism (**Dlm**): The delay mechanism used for the port. Possible values are:
    - *e2e*: End to end delay measurement.
    - *p2p*: Peer to peer delay measurement.

  Can be defined per port in an Ordinary or Boundary clock. In a transparent clock all ports use the same delay mechanism, determined by the clock type.

- **MPR**: The interval for issuing Delay_Req messages for the port in e2e mode. This value is announced from the master to the slave in an announce message. The value is reflected in the MDR field in the Slave. The interval for issuing Pdelay_Req messages for the port in P2P mode.

Note The interpretation of this parameter has changed from release 2.40. In earlier versions, the value was interpreted relative to the Sync interval, this was a violation of the standard, so now the value is interpreted as an interval that is, MPR = 0 => 1 Delay_Req pr sec, independent of the Sync rate. Range is -7 to 5.

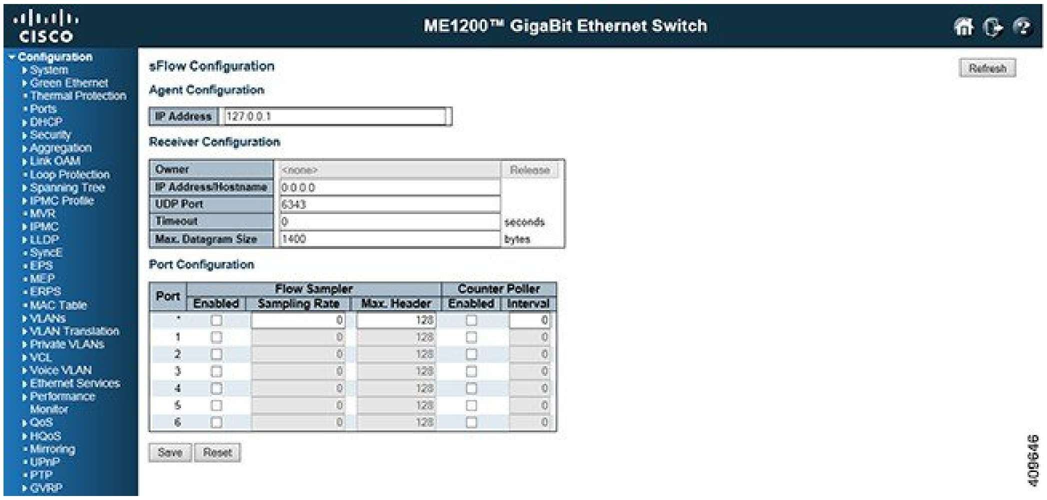
- **Delay Asymmetry**: If the transmission delay for a link in not symmetric, the asymmetry can be configured here, see IEEE 1588 Section 7.4.2 Communication path asymmetry. Range is -100000 to 100000.
- **Ingress latency**: Ingress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2. Range is -100000 to 100000.
- **Egress Latency**: Egress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2. Range is -100000 to 100000.
- **Version**: The current implementation only supports PTP version 2.

CHAPTER 27

Configuring sFlow

sFlow Configuration

This feature allows you to configure sFlow. The configuration is divided into two parts: Configuration of the sFlow receiver (also called sFlow collector) and configuration of per-port flow and counter samplers. sFlow configuration is not persisted to non-volatile memory, which means that a reboot will disable sFlow sampling.



sFlow Configuration

Agent Configuration

IP Address	127.0.0.1

Receiver Configuration

Owner	<none>	Release
IP Address/Hostname	0.0.0.0	
UDP Port	6343	
Timeout	0	seconds
Max. Datagram Size	1400	bytes

Port Configuration

Port	Flow Sampler			Counter Poller	
	Enabled	Sampling Rate	Max. Header	Enabled	Interval
*	□	0	128	□	0
1	□	0	128	□	0
2	□	0	128	□	0
3	□	0	128	□	0
4	□	0	128	□	0
5	□	0	128	□	0
6	□	0	128	□	0

Agent Configuration

- **IP Address**: The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time. Both IPv4 and IPv6 addresses are supported.

Receiver Configuration

- **Owner**: Basically, sFlow can be configured in two ways: Through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:

  - If sFlow is currently unconfigured/unclaimed, **Owner** contains <*none*>.
  - If sFlow is currently configured through Web or CLI, **Owner** contains <*Configured through local management*>.
  - If sFlow is currently configured through SNMP, **Owner** contains a string identifying the sFlow receiver.

  If sFlow is configured through SNMP, all controls - except for the **Release**-button - are disabled to avoid inadvertent reconfiguration. The **Release** button allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed.

  If configured through SNMP, the release must be confirmed (a confirmation request will appear).

- **IP Address/Hostname**: The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.
- **UDP Port**: The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.
- **Timeout**: The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings. Valid range is 0 to 2147483647 seconds.
- **Max. Datagram Size**: The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.

Port Configuration

- **Port**: The port number for which the configuration below applies.
- **Flow Sampler Enabled**: Enables or disables flow sampling on this port.
- **Flow Sampler Sampling Rate**: The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted or received on the port.

  Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field. Valid range is 1 to 4294967295

- **Flow Sampler Max. Header**: The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes.

  If the maximum datagram size does not take into account the maximum header size, samples may be dropped.

- **Counter Poller Enabled**: Enables or disables counter polling on this port.
- **Counter Poller Interval**: With counter polling enabled, this specifies the interval - in seconds - between counter poller samples. Valid range is 1 to 3600 seconds.

Related Topics

Monitoring sFlow, on page 239
sFlow Statistics, on page 239

CHAPTER 28

Configuring Traffic Test

The Traffic Test feature available on the ME 1200 Web GUI allows you to configure Traffic Test Loop instances for the ME 1200 switch.

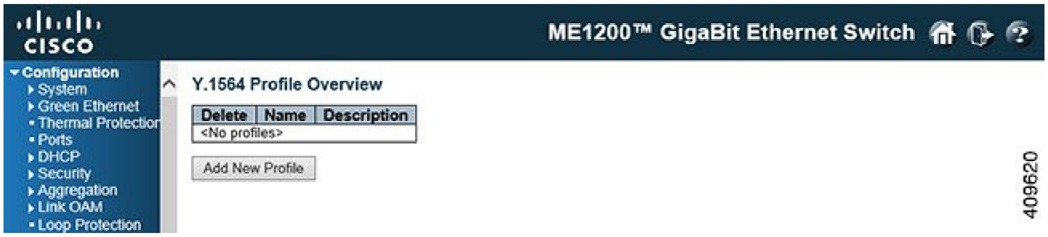
Y.1564

Y.1564 Profile Overview

Y.1564 is an Ethernet service activation to test Ethernet Virtual Connections (EVCs). One single EVC is a collection of one or more ordered set of rules, known as ECEs. Each ECE describes matching criteria for traffic arriving at the UNI. For example, an Ethernet Virtual Private Line (EVPL) ECE matches a particular VLAN ID.

The ECE defines a set of actions. In relation to Y.1564, the most important action is the policer it maps to. Policers are configured separately, and multiple ECEs may point to the same physical policer, sharing the bandwidth set by the policer. Policers can also be attached to an EVC, and the ECE can be configured to use the EVC policer.

To execute a Y.1564 test, a set of Y.1564-specific configuration along with information about which EVC or ECE to test is needed. The Y.1564-specific configuration is independent of the EVC/ECE to test, and is called a **profile**. The profile can be used multiple times as input configuration to test EVCs/ECEs as they are created. The result of executing a profile is called a **report**. Up to 16 profiles and 10 reports can be stored on the switch.



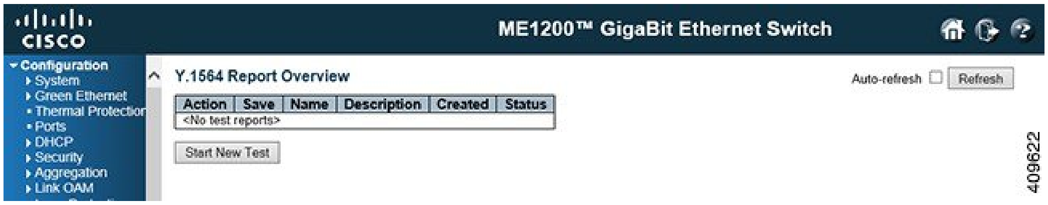
Y.1564 Profile Overview

Delete	Name	Description
<No profiles>		

This option provides an overview of the defined profiles along with options for editing and deleting them and creating new profiles. If no profiles are currently defined, the table contains one line stating **<No profiles>**. Otherwise there is a table row for each defined profile with these three elements:

- **Delete**: Click **Delete** to delete the profile in question.
- **Name**: A unique name identifying the profile. Click the name to edit the profile.
- **Description**: The profile's description as entered in the profile editor, which is activated by clicking the name of the profile.
- **Add New Profile**: This button is grayed out if the maximum number of profiles is already defined.

Y.1564 Report Overview



Y.1564 Report Overview

Action	Save	Name	Description	Created	Status
<No test reports>					

This option provides an overview of the stored reports along with options for deleting, downloading, and viewing them. Initiation of execution of an EVC is also handled through this option. If no reports are currently stored, the table contains one line stating *<No test reports>*. Otherwise, there is a table row for each test report, each containing these elements:

- **Action**: If a test is executed, a **Stop** button is shown. Clicking **Stop** causes a request to be sent to cancel the execution. During this cancellation, the button is disabled. At most one test can be executed at a time.

  Once execution of a test is complete, the resulting report is persisted to non-volatile memory. Up to 10 reports can be persisted. New reports will replace the oldest. Only reports stored in non-volatile memory can be erased. This is done with the **Delete** button.
- **Save**: Test reports can be downloaded and stored on the local computer with the use of the **Save** button. The suggested file name will be the report name concatenated with .txt.
- **Name**: A unique name identifying the report.
- **Description**: The description assigned to the report as entered on the test execution page, invoked with **Start New Test**.
- **Created**: The date and time at which execution started.

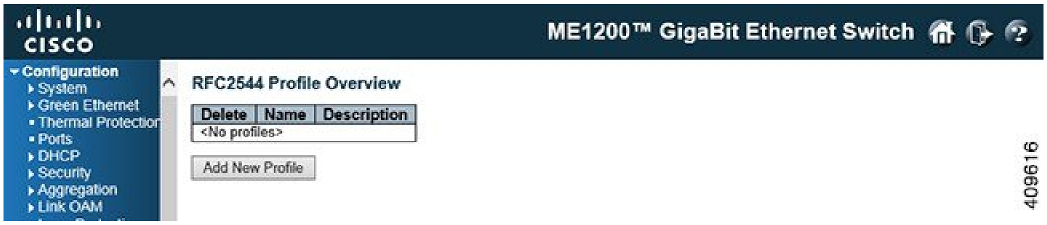
- **Status**: The current status of executing a test:
    - *Inactive*: Test just initiated, but not started. This is a transitional state that is unlikely to be noticed.
    - *Executing*: Test is currently executing. At most one test can execute at a time.
    - *Cancelling*: Test has just been stopped by the user. This is a transitional state that is unlikely to be noticed.
    - *Cancelled*: Test was stopped by the user and report is stored in non-volatile memory.
    - *Passed*: Test passed successfully and report is stored in non-volatile memory.
    - *Failed*: Test failed execution and report is stored in non-volatile memory. Details as to why the test failed are embedded in the report.

RFC2544

RFC2544 Profile Overview

RFC2544 is a benchmark testing tool that allows for testing an ethernet service connection end-to-end w.r.t. various key parameters. Each test configuration is called a **profile**, and each result of executing the profile is called a **report**. You can store up to 16 profiles and 10 reports. Executing a profile causes the switch (near end) to generate and transmit frames at certain rates on the configured egress port. The remote end is supposed to loop these frames while swapping source and destination MAC addresses. The looped frames are then expected to arrive at the same port as they egressed at the near end. The switch that generated the frames can therefore assess whether an ethernet service connection meets the SLA.

Note This switch supports the near-end functionality only (generation + check of frames). Remote end functionality (loop + MAC address swap) is not supported.



RFC2544 Profile Overview

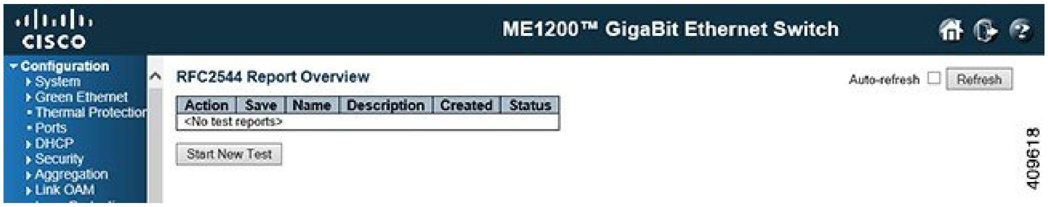
Delete	Name	Description
<No profiles>		

This option provides an overview of the defined profiles along with options for editing and deleting them and creating new. If no profiles are currently defined, the table contains one line stating *<No profiles>*. Otherwise there is a table row for each defined profile with these three elements:

- **Delete**: Delete the profile in question.
- **Name**: A unique name identifying the profile.
- **Description**: The profile's description as entered in the profile editor, which is activated by clicking the name of the profile.

- **Add New Profile**: This button is grayed out if the maximum number of profiles is already defined.

RFC2544 Report Overview



RFC2544 Report Overview

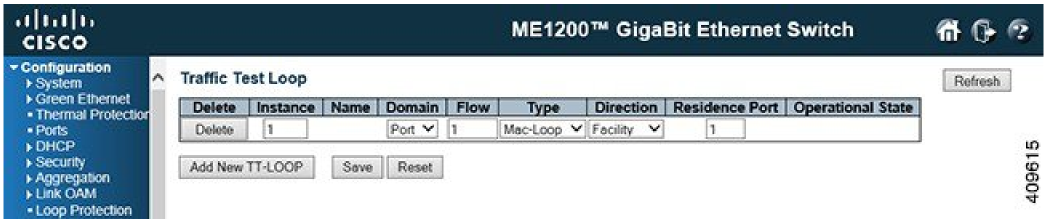
Action	Save	Name	Description	Created	Status
<No test reports>					

This option provides an overview of the stored reports along with options for deleting, downloading, and viewing them. Initiation of execution of a profile is also handled through this option. If no reports are currently stored, the table contains one line stating <*No test reports*>. Otherwise there is a table row for each test report, each containing these elements:

- **Action**: If a test is currently being executed, a **Stop** button is shown. Clicking **Stop** cancel the execution of the test. During this cancellation, the button will be disabled. At the most, one test can execute at a time.
- **Save**: Test reports can be downloaded and stored on the local computer. The suggested file name will be the report name concatenated with ".txt".
- **Name**: A unique name identifying the report.
- **Description**: The description assigned to the report as entered on the test execution page, invoked with the **Start New test** button.
- **Created**: The date and time at which execution started.
- **Status**: The current status of executing a test:
  - *Inactive*: Test just initiated, but not started. This is a transitional state that is unlikely to be noticed.
  - *Executing*: Test is currently executing. At most one test can execute at a time.
  - *Cancelling*: Test has just been stopped by the user. This is a transitional state that is unlikely to be noticed.
  - *Cancelled*: Test was stopped by the user and report is stored in non-volatile memory.
  - *Passed*: Test passed successfully and reports is stored in non-volatile memory.
  - *Failed*: Test failed execution and report is stored in non-volatile memory. Details as to why the test failed are embedded in the report.

TT-LOOP

This option allows you to create the Traffic Test Loop (TT-LOOP) instances.



Traffic Test Loop

Delete	Instance	Name	Domain	Flow	Type	Direction	Residence Port	Operational State
Delete	1		Port	1	Mac-Loop	Facility	1	

Add New TT-LOOP   Save   Reset

- **Delete**: This box is used to mark a TT-LOOP for deletion in next Save operation.
- **Instance**: The ID of the TT-LOOP. Click on the ID of a TT-LOOP to enter the configuration page.
- **Name**: This is a configurable name of the instance.
- **Domain**: Currently VLAN domain is not supported.
  - *Port*: This is a TT-LOOP in the Port Domain.
  - *Evc*: This is a TT-LOOP in the EVC Domain. 'Flow' is an EVC. The EVC must be created.
  - *VLAN*: This is a TT-LOOP in the VLAN Domain. 'Flow' is a VLAN. In case of Up-TT-LOOP the VLAN must be created.
- **Flow**: The flow instance number related to this TT-LOOP instance - depending on the 'Domain'.
- **Type**: Currently OAM Loop is only supported in EVC domain.
  - *Mac-loop*: This TT-LOOP is the MAC looping type. All frames in the flow is looped with MAC swap.
  - *Oam-loop*: This TT-LOOP is the OAM looping type. Is Y.1731 OAM aware and is looping LBM->LBR and DMM->DMR.
- **Direction**: Currently Terminal Loop is only supported in EVC domain.
  - *Facility*: This TT-LOOP is pointing out to the port. Looping is done from ingress to egress.
  - *Terminal*: This TT-LOOP is pointing into the forwarding plane. Looping is done from egress to ingress.
- **Residence Port**: The port where TT-LOOP is resident - see 'Direction'. For an EVC TT-LOOP the port must be a port in the EVC. For a VLAN TT-LOOP the port must be a VLAN member.
- **Operational State**
  - *Up*: Instance Operational State is UP - all resources are available and allocated.
  - *Down*: Instance Operational State is DOWN - not all resources are available or administrative state is disabled.

CHAPTER 29

Configuring Traffic Test Loops

Configuring Traffic Test Loops

This chapter describes the Traffic Test Loop feature and how to use it.

A traffic test loop can be used to return selected Ethernet frames in the direction from which they came. This feature is intended for Service Activation Testing (SAT) and troubleshooting for point-to-point and multipoint services across multiple Carrier Ethernet Networks (CENs).

Traffic Test Loop Function

Loop Instances

A single system can contain several loop instances. Only four instances can however be active at any given point in time.

Loop Modes

The system supports two different loop modes:

- Static Loopback
- Latching Loopback (as specified in MEF 46)

The Static Loopback mode is fully configured and controlled by management actions. Once configured and activated the loop will operate until explicitly changed or deactivated by another management operation.

The Latching Loopback mode combines management operations and OAM frame exchange to enable operational control of the loop from a remote system without management interface access. The loop must be initially provisioned by the management interface but it can be activated and deactivated using a standard Y.1731 OAM frame sequence.

The Latching Loopback mode conforms to the MEF 46 specification with the exceptions listed in the MEF 46 Non-Conformance Statement section.

Both modes are configured in a similar way. Since the static loops were added first the latching loop function has been implemented as an "add-on" function to the existing loop function.

Loop Domain

A loop instance must be created within one of the following domains. The domain determines which frames to loop.

Domain	Frames to Loop
Port	All ingress or egress frames on the selected port.
VLAN	All ingress or egress frames on the selected port with the configured VLAN.
EVC	All ingress or egress frames classified as belonging to the EVC.
EVC Subscriber	All ingress or egress frames classified as belonging to the EVC and located in the subscriber domain of the EVC and tagged with an optional Subscriber VID.

Loop Type

The loop type determines which type of frames to loop and the action performed on the looped frames.

Domain	Frames to Loop
MAC Loop	All frames in the flow are looped. The source MAC (SMAC) address and destination MAC (DMAC) addresses are swapped.
OAM Loop	Only Y.1731 OAM Loopback Messages (LBM) and Delay Measurement Messages (DMM) frames are looped. LBM frames are converted to LBR frames and DMM frames are converted to DMR frames. **Note** The OAM loop type is only supported for static loops and not for latching loops.

Loop Direction

The loop can be configured with two different directions.

Direction	Description
Facility	This loop is pointing out to the port. Looping is done from ingress to egress.
Terminal	This loop is pointing into the forwarding plane. Looping is done from egress to ingress.

Loop Residence Port

Any loop instance must be configured with a residence port regardless of the domain and direction settings. The residence port indicates the point in the system where frames that would otherwise have been forwarded is returned to the sender.

The valid choices of residence port depend on the domain and direction settings.

Warning Ignore

When enabling a Port domain facility loop all frames on the port will be looped including any management IP frames - management access will be lost on this port. To ensure that the user is aware of these consequences a warning is printed and the loop is not enabled. To enable the loop, the user must append the ICLI command with the keyword 'warning-ignore'.

EVC Domain Latching Loop Overview

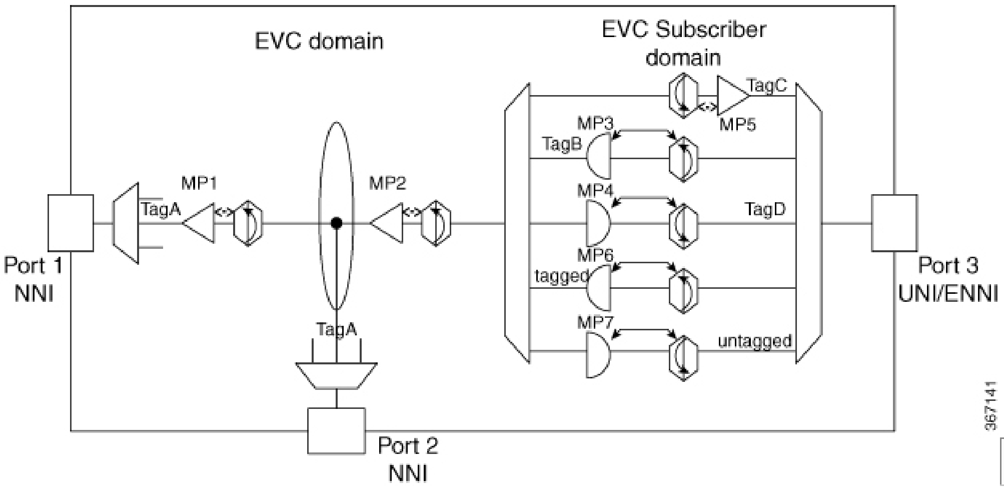
The Port and VLAN loop domains are rather simple to understand and setup. But the EVC and EVC Subscriber domains are a bit more complex, especially when used in conjunction with the Latching Loopback mode.

The figure below shows a generalized view of a switch, together with the various possible locations for a latching loop instance in the EVC and EVC Subscriber domains.

The vertical ellipsis in the middle represents the actual layer-2 MAC/VLAN switch function. The small rectangles at the edge of the larger box represents ports on the switch. In case of an EVC the ports are marked with their role (NNI or UNI/ENNI).

The tag notation is explained in the figure below:

Figure 1: EVC Domain Latching Loops



Tag notation:

- TagA is the first tag on NNI.
- TabB is the second tag on NNI.
- TagC and TagD are first tag on UNI/ENNI.

MEP/MIP notation:

- MP1 is an EVC Down-MEP on NNI and the LLFS is TagA.
- MP5 is a Down-MEP on UNI/ENNI and the LLFS is TagC.
- MP4 is a Down-MIP on UNI/ENNI and the LLFS is TagD.
- MP7 is a Down-MIP on UNI/ENNI and the LLFS is Untagged.
- MP2 is an Up-MEP on UNI and the LLFS is TagA.
- MP3 is an Up-MIP on UNI and the LLFS is TagA+TagB.
- MP6 is an Up-MIP on UNI and the LLFS is TagA+Untagged.

Valid Feature Combinations

This table shows the supported loop paramaters combinations.

Domain	Static Loop		Latching Loop	
	Facility	Terminal	Facility	Terminal
Port	Supported	Not Applicable	Not Applicable	Not Applicable

Domain	Static Loop		Latching Loop	
VLAN	Supported	Not Applicable	Supported	Not Applicable
EVC Subscriber	Supported	Supported	Supported	Supported

Valid Residence Port Types

This table shows the type of EVC ports that can be used as a residence port depending on the other settings.

Note The table is relevant only for EVC domain loops.

Domain	Direction	Valid Port Types
EVC	Facility	NNI ports
	Terminal	UNI ports
EVC Subscriber	Facility	UNI ports
	Terminal	UNI ports

MEF 46 Non-Conformance Statement

The system provides a Latching Loopback function which is fully MEF 46 conformant with the following exceptions:

- On a Serval-1 system a Terminal loop will loop the whole residence port due to limitations in the system hardware. This means that other flows using the same port will be affected when the loop is activated.
- A single latching loopback instance can only reference a single Maintenance Point (MEP or MIP).

Configuration Examples

The following sections describe various ICLI configuration examples based on the feature description section.

It is recommended to perform a restore to default operation before starting to configure any of the examples in the following sections.

```
# reload defaults
#
```

Note the following points with respect to the syntax:

- Lines that starts with an exclamation mark denotes an explanatory comment. You do not have to enter these in the ICLI console.

- Text in bold denote user input. These are the commands you need to type.
- Other text denotes command response from the system.
- Blank lines are occasionally inserted to increase readability.
- Wrapped CLI command lines (i.e. user input) will be shown with a '>' marker at the start of the wrapped text.
- Truncated CLI output lines will be shown with a '<...>' marker at the end of the line.

Static Loopback

This section contains examples of how to set up a static loop.

Port Facility Loop

This example describes how to create a simple static loop for port 1/1. The loop has type = MAC-Loop. The direction is set to facility, which means that all frames received by the port are looped back out on the port. The loop instance is given instance number '1'.

```
! Enter configuration mode
# configure terminal

! Create the loop
(config)# traffic-test-loop 1 type mac-loop interface GigabitEthernet 1/1 direction facility
> domain port admin-state disabled

! Give the loop a name
(config)# traffic-test-loop 1 name MyLoop

! The loop instance is now created but not active.
! Activate the loop
(config)# traffic-test-loop 1 admin-state enabled warning-ignore

! The loop instance is now active and will loop frames. Without 'warning-ignore' a warning
 is given and the loop is not active.

! Leave configuration mode and view the loop state
(config)# exit
# show traffic-test-loop 1

Traffic Test Loop:
 inst    name      type   opctrl   direction   domain   flow                 port <...>
    1  MyLoop  mac-loop   static    facility     port      -    GigabitEthernet 1/1 <...>

! Enter configuration mode again
# configure terminal

! Deactivate the loop
(config)# traffic-test-loop 1 admin-state disabled

! Remove the loop instance
(config)# no traffic-test-loop 1
```

EVC Terminal Loop

This example shows how to create a static terminal loop of type MAC-Loop in the EVC domain.

The example assumes that an EVC has already been created with EVC ID = 1, and with port 1/2 as a UNI port.

```
! Enter configuration mode
# configure terminal

! Create the loop
(config)# traffic-test-loop 1 type mac-loop interface GigabitEthernet 1/2 direction terminal
 domain evc 1 admin-state disabled

! Give the loop a name
(config)# traffic-test-loop 1 name MyEVCLoop

! Activate the loop
(config)# traffic-test-loop 1 admin-state enabled

! The loop instance is now active and will loop frames.

! Leave configuration mode and view the loop state
(config)# exit
# show traffic-test-loop 1

Traffic Test Loop:
 inst  name               type   opctrl  direction  domain   flow                 port <...>

    1  TRAFFIC_<...>  mac-loop   static   terminal     evc      1  GigabitEthernet 1/2 <...>

! Enter configuration mode again
# configure terminal

! Remove the loop instance (not strictly necessary to deactivate first)
(config)# no traffic-test-loop 1
```

Latching Loop

This section contains examples of how to set up a latching loop.

Note When setting up a latching loop instance it is very important that the instance is initially created with admin-state = disabled and that the admin-state is not set to enabled until the latching loop function has been configured for the instance. Otherwise the loop will behave as a static loop and will immediately start to loop frames!

VLAN Facility Loop

This example shows how to create a latching loop for VLAN 200 on port 1/1. The loop will have type = MAC-Loop. The direction will be set to facility. The latching loop OAM frame handling will be enabled using a MEP with instance ID = 1 and will be provisioned with a source MAC (SMAC) filter = 00:11:22:33:44:55. Refer to [AN1105] for details on how to create MEPs.

With this configuration, only frames arriving on port 1/1 with VLAN tag 200 and with the specified SMAC address will be looped.

The example also shows how to inspect the state of an actively looping instance.

```
! Enter configuration mode
# configure terminal

! Create the MEP used for handling the latching loop OAM frames
(config)# mep 1 down domain vlan flow 200 level 0 interface GigabitEthernet 1/1
```

```
! Create the loop
(config)# traffic-test-loop 1 type mac-loop interface GigabitEthernet 1/1 direction facility
> domain vlan 200 admin-state disabled

! Give the loop a name
(config)# traffic-test-loop 1 name MyLlVlanLoop

! Setup the Latching Loop function
(config)# traffic-test-loop 1 ll mep 1 smac 00:11:22:33:44:55

! Enable the loop
(config)# traffic-test-loop 1 admin-state enabled

! The loop instance is now enabled but not active, i.e. it will not start to loop
! until it receives a valid Latching Loop LLM "Activate" OAM frame.

! Leave configuration mode and view the basic loop state
(config)# exit
# show traffic-test-loop 1

Traffic Test Loop:
  inst          name     type  opctrl  direction  domain  flow                   port <...>

     1 MyLlVlanLoop  mac-loop latch-l   facility    vlan   200    GigabitEthernet 1/1 <...>

! show the specific latching loop state
# show traffic-test-loop 1 ll

Traffic Test Latching Loop:
  inst   mep               smac      admin          oper     timer
     1     1  00-11-22-33-44-55    enabled      inactive        0s

! Note that the "oper" state is 'inactive' and that the "timer" value is 0s which
! indicate that the loop is not active and it not looping traffic.

! Ensure that the latching loop is activated using an LLM OAM packet exchange
! using a remote system. Set the expiry timer to e.g. 30 seconds.

! show the specific latching loop state
# show traffic-test-loop 1 ll

Traffic Test Latching Loop:
  inst   mep               smac      admin          oper     timer
     1     1  00-11-22-33-44-55    enabled            up       27s

! Wait for at least 30 seconds and check the state again.
# show traffic-test-loop 1 ll

Traffic Test Latching Loop:
  inst   mep               smac      admin          oper     timer
     1     1  00-11-22-33-44-55    enabled      inactive        0s

! Remove the loop instance
(config)# no traffic-test-loop 1
```

EVC Subscriber Facility Loop

This example shows how to create a latching loop in the subscriber domain of an EVC using C-VID = 10. The example assumes that an EVC has already been created with EVC ID = 1, and with port 1/2 as a UNI port. Please refer to [AN1142] for details on how to create an EVC.

The latching loop OAM frame handling will be enabled using a MIP with instance ID = 1 and will be provisioned with a source MAC (SMAC) filter = 00:11:22:33:44:55. Refer to [AN1105] for details on how to create MEPs.

With this configuration, only frames arriving on port 1/2 with C-VID = 10 and with the specified SMAC address will be looped.

```
! Enter configuration mode
# configure terminal

! Create the MIP used for handling the latching loop OAM frames
(config)# mep 1 mip down domain evc vid 10 flow 1 level 4 interface GigabitEthernet ½

! Create the loop
(config)# traffic-test-loop 1 type mac-loop interface GigabitEthernet 1/1 direction facility

> domain evc 1 subscriber vid 10 admin-state disabled

! Setup the Latching Loop function
(config)# traffic-test-loop 1 ll mep 1 smac 00:11:22:33:44:55

! Enable the loop
(config)# traffic-test-loop 1 admin-state enabled

! The loop instance is now enabled but not active, i.e. it will not start to loop
! until it receives a valid Latching Loop LLM "Activate" OAM frame.
```

User Interface Reference

This section describes all configurable and viewable parameters for the Traffic Test Loop function.

The content of this section applies to both static and latching loopback modes.

iCLI Interface

All Traffic Test Loop operations use the traffic-test-loop command name.

Show Command

The command syntax for viewing settings and status is as follows:

```
show traffic-test-loop [ <inst> ] [ ll ]
```

Argument	Explanation
<inst>	This optional argument is the 1-offset identifier number assigned to the loop instance. If this is omitted, all instances will be shown.
ll	This optional argument will display special configuration and state for a Latching Loopback loop. If this is omitted only the common configuration and state will be shown, regardless of the mode of the loop.

Main Configuration Command

The main command syntax for configuring loops is as follows:

```
traffic-test-loop <inst>
type { mac-loop | { oam-loop [ level <level> ] } }
  interface <port_type> <port>
direction { terminal | facility }
domain {
   port |
   { evc <evc_id> [ subscriber { all | untagged | { vid <sub_vid> } } ] } |
   { vlan <vlan_vid> }
 }
  [ admin-state { enabled | disabled } ]
[ warning-ignore ]
```

Argument	Description
<inst>	This argument is the 1-offset identifier number assigned by the user to the loop instance when it is created.
type	Selects the type of the loop as explained in section 2.1.4. If the type is set to "OAM Loop" then a MEG level value must also be provided.
interface	Selects the residence port for the loop.
direction	Selects the direction of the loop.
domain	Selects the domain for the loop.
evc_id	The ID of the EVC if the domain is set to "EVC". The EVC must exist when activating the loop.
subscriber	Optional EVC Subscriber settings if the domain is set to "EVC".
all	All frames in the EVC subscriber domain will be looped.
untagged	Only untagged frames in the EVC subscriber domain will be looped.
vid <sub_vid>	Only frames tagged with subscriber VID <sub_vid> in the EVC subscriber domain will be looped.
vlan_vid	The VLAN VID to use if the domain is set to "VLAN".
admin-state	Controls the administrative state of the loop. The default value is "disabled".
warning-ignore	Ignore the warning when enabling a Port Domain facility loop. The loop is enabled.

Naming Loop Instance

This sub-command can be used to change the display name of an existing loop instance.

```
traffic-test-loop <inst> name <name>
```

Argument	Description
<inst>	This argument is the 1-offset identifier number assigned by the user to the loop instance when it is created.
name	A display name to help the user identify the loop instance. The name can at most contain 32 characters and may not contain spaces.

Controlling Subscriber Domain Settings

The EVC subscriber settings can also be (re-)configured using a separate command.

```
traffic-test-loop <inst> subscriber [ all | untagged | { vid <vlan_id> } ]
```

Controlling Latching Loopback Mode

A loop instance is by default created as a static loop but the latching loop mode can be enabled after initial creation with this separate command.

```
traffic-test-loop <inst> ll mep <mep_id> smac <mac_address>
```

Argument	Description
<inst>	This argument is the 1-offset identifier number assigned by the user to the loop instance when it is created.
ll	Indicate that the remaining command arguments are related to the latching loop mode.
mep <mep_id>	Indicate the MEP or MIP instance which shall be responsible for processing Latching Loopback OAM frames (LLM/LLR) for the loop. This MEP/MIP must be created on the residence port defined for the loop. It must also be assigned to a similar domain as the loop. **Note** MEP instances must be used for Port and VLAN domain loop and also for main EVC domain loops. MIP instances can be used for EVC Subscriber domain loops.

Argument	Description
smac <mac_address>	The Source MAC (SMAC) filter to use for the loop. This is used to select frames to include in the loop but LLM OAM frames sent to the loop must also use this SMAC address.

Controlling Administrative State

The loop administrative state can be set in the main configuration command, but it can also be controlled for an existing loop instance with this separate command.

```
traffic-test-loop <inst> admin-state { enabled | disabled }
```

Note When setting up a latching loop instance it is very important that the instance is initially created with admin-state = disabled (the default value) and that the admin-state is not set to enabled until the latching loop function has been enabled for the instance. Otherwise, the loop immediately starts to loop frames!

Web Interface

The web interface provides the same configuration options for the Traffic Test Loop function as the ICLI interface described in section . Please refer to this section for a detailed description of the various parameters.

The Traffic Test Loop function can be reached in the web interface using the menu on the left as follows:

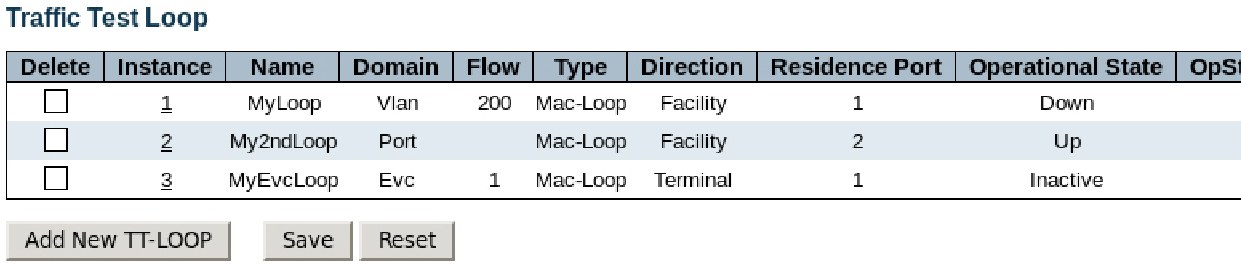
- Expand the Top-most Configuration level
- Expand the Traffic Test level (located near the bottom)
- Select the Loop menu entry (see the screenshot to the right).

The main overview page is then shown.

Viewing Existing Loop Instances

The main overview page displays all configured loop instances together with their main configuration and current state.

Figure 2: Main Loop Overview



Traffic Test Loop

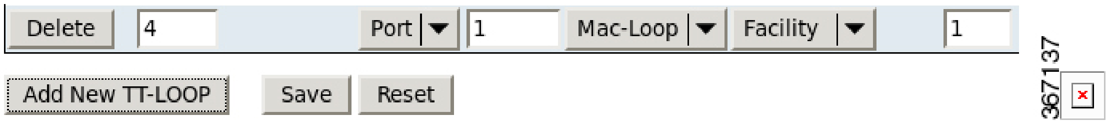
Delete	Instance	Name	Domain	Flow	Type	Direction	Residence Port	Operational State	OpSt
□	1	MyLoop	Vlan	200	Mac-Loop	Facility	1	Down	
□	2	My2ndLoop	Port		Mac-Loop	Facility	2	Up	
□	3	MyEvcLoop	Evc	1	Mac-Loop	Terminal	1	Inactive	

Creating a New Loop

To create a new loop instance:

1 Click **Add New TT-LOOP**. A new row is inserted in the overview table.

Figure 3: Creating a New Loop



Delete	4	Port	1	Mac-Loop	Facility	1

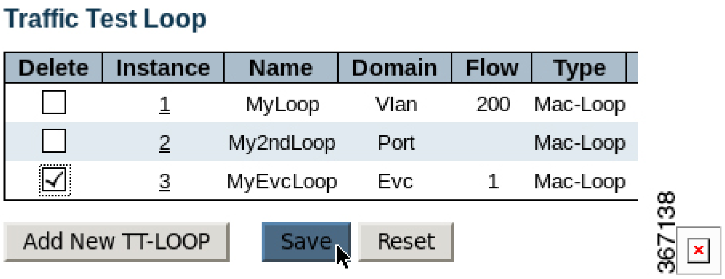
2 Fill in the parameters for the loop and click **Save**.

3 To cancel the loop creation, click **Reset**. Alternatively, click **Delete** in the first column.

Deleting a Loop Instance

To delete one or more existing loop instances, select the checkbox in the first column of the loop row(s) you want to delete and click **Save**.

Figure 4: Deleting a Loop Instance



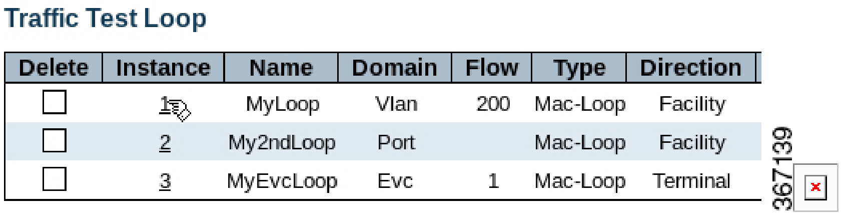
Traffic Test Loop

Delete	Instance	Name	Domain	Flow	Type
□	1	MyLoop	Vlan	200	Mac-Loop
□	2	My2ndLoop	Port		Mac-Loop
☑	3	MyEvcLoop	Evc	1	Mac-Loop

Modifying a Loop Instance

To change the settings of an existing loop instance, click the hyperlinked instance number in the Instance column.

Figure 5: Modifying a Loop Instance



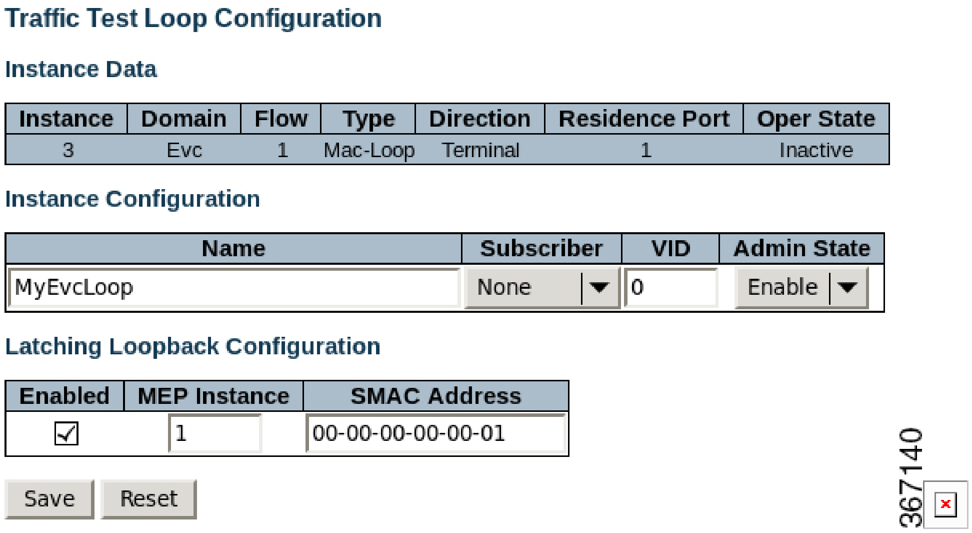
Traffic Test Loop

Delete	Instance	Name	Domain	Flow	Type	Direction
□	1	MyLoop	Vlan	200	Mac-Loop	Facility
□	2	My2ndLoop	Port		Mac-Loop	Facility
□	3	MyEvcLoop	Evc	1	Mac-Loop	Terminal

The following loop parameters cannot be changed after they are created in the Web interface:

- Instance number
- Domain
- Flow association
- Type
- Direction
- Residence port

Figure 6: Loop Parameters



Traffic Test Loop Configuration

Instance Data

Instance	Domain	Flow	Type	Direction	Residence Port	Oper State
3	Evc	1	Mac-Loop	Terminal	1	Inactive

Instance Configuration

Name	Subscriber	VID	Admin State
MyEvcLoop	None	0	Enable

Latching Loopback Configuration

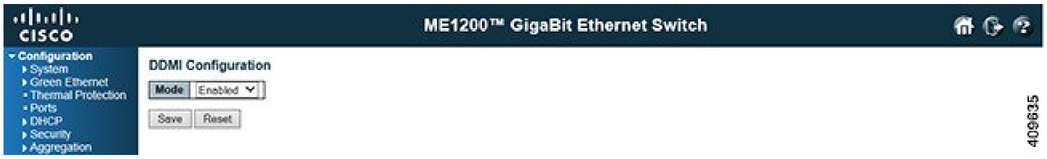
Enabled	MEP Instance	SMAC Address
☑	1	00-00-00-00-00-01

CHAPTER 30

Configuring DDMI

DDMI Configuration

This feature allows you to configure DDMI.



DDMI Configuration

Mode	Enabled

Mode: Indicates the DDMI mode operation. Possible modes are:

- ***Enabled***: Enables DDMI mode operation.
- ***Disabled***: Disables DDMI mode operation.

Related Topics

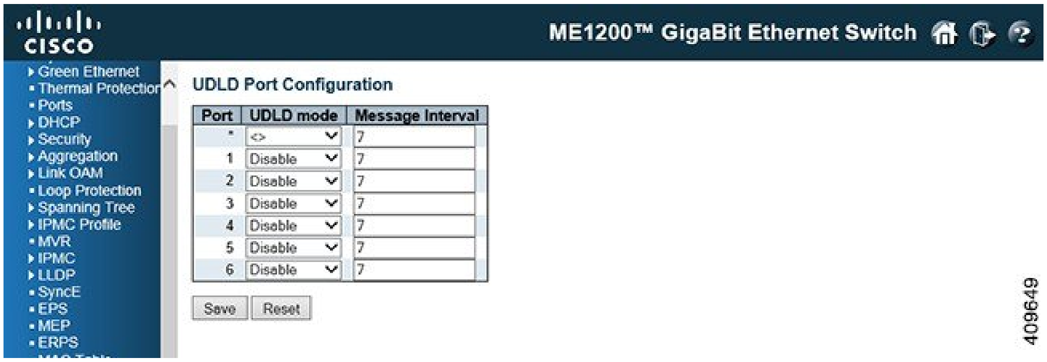
Monitoring DDMI, on page 241

CHAPTER 31

Configuring UDLD

UDLD Port Configuration

This feature allows you to inspect the current UDLD configurations and change them.



UDLD Port Configuration

Port	UDLD mode	Message Interval
*	<>	7
1	Disable	7
2	Disable	7
3	Disable	7
4	Disable	7
5	Disable	7
6	Disable	7

- **Port**: Port number of the switch.
- **UDLD Mode**: Configures the UDLD mode on a port. Valid values are Disable, Normal and Aggressive. Default mode is Disable.
  - *Disable*: In disabled mode, UDLD functionality does not exist on the port.
  - *Normal*: In normal mode, if the link state of the port was determined to be unidirectional, it will not affect the port state.
  - *Aggressive*: In aggressive mode, unidirectional detected ports will get shutdown. To bring back the ports up, need to disable UDLD on that port.
- **Message Interval**: Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is from 7 to 90 seconds (Default value is 7 seconds. Currently default time interval is supported, due to lack of detailed information in RFC 5171).

Related Topics

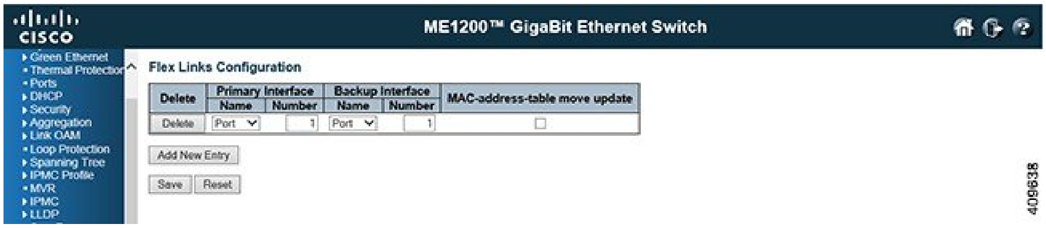
Monitoring UDLD, on page 243

CHAPTER 32

Configuring Flex Links

Flex Links Configuration

The Flex Links pairs and their mac-address-move update transmit feature can be configured here. This option allows adding, editing and deleting a port or a port channel as backup for a primary interface, and enable or disable the mac-address-move update transmit feature for the flex links pair. Disable spanning-tree for flex links pair to function properly.



Flex Links Configuration

Delete	Primary Interface		Backup Interface		MAC-address-table move update
	Name	Number	Name	Number	
Delete	Port	1	Port	1	□

- **Delete**: To delete an existing flex links pair, check this check box and click **Save**. The entry will be deleted from the switch.
- **Primary Interface**: This defines the primary interface in **Name** and **Number**. Name can be chosen as a port or LLAG (port channel), and Number can be a valid ID. For example, for port number can be 1 to 6, and LLAG number can be any existing LLAG group id.

> **Note** After adding a primary interface, the primary interface entry can only be deleted but not edited.

- **Backup Interface**: This defines the backup interface in **Name** and **Number**, as described in primary interface. The backup interface entry can be edited
- **MAC-address-table move update**: A check box for enabling or disabling the mac-address-move update transmit feature for the particular flex links entry. To enable the mac-address-move update transmit feature, check the check box. The check box is unchecked by default.

- **Add New Entry**: Click this button to add a new Flex Links entry. An empty row is added to the table, and the flex links pair can be configured as needed. Legal values for a interface port number are 1 through 6. Legal values for a interface LLAG number are any existing LLAG group ids.

  An entry with any members duplicating the existing entries in either port interface or LLAG groups will not be added when you click **Save**. The port interface that is included in an LLAG group is not allowed to be used alone.

  The Delete button can be used to undo the addition of new entries. The maximum possible entries number are limited to port array size.

Related Topics

Monitoring Flex Links, on page 245

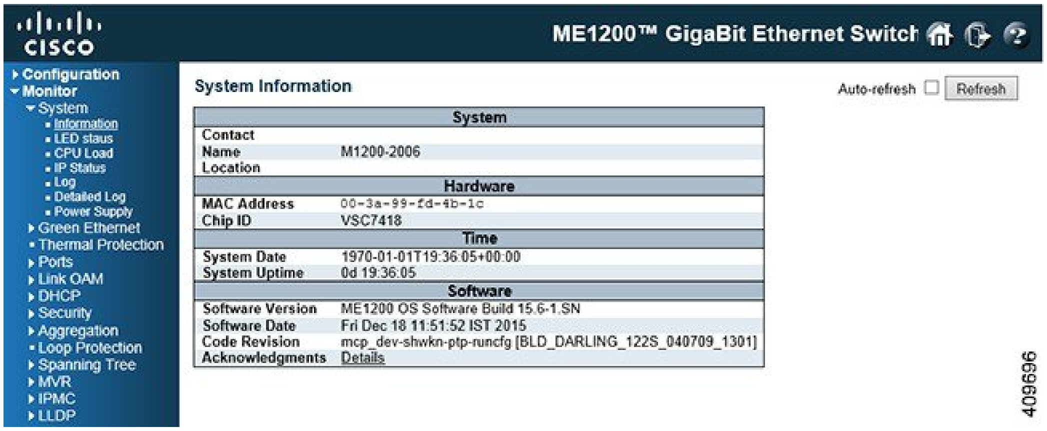
CHAPTER 33

Monitoring System

The System feature available on the ME 1200 Web GUI allows you to monitor your computer's configuration information.

System Information

This option allows you to view the switch system information.



System Information

System	
Contact	
Name	M1200-2006
Location	
Hardware	
MAC Address	00-3a-99-fd-4b-1c
Chip ID	VSC7418
Time	
System Date	1970-01-01T19:36:05+00:00
System Uptime	0d 19:36:05
Software	
Software Version	ME1200 OS Software Build 15.6-1.SN
Software Date	Fri Dec 18 11:51:52 IST 2015
Code Revision	mcp_dev-shwkn-ptp-runcfg [BLD_DARLING_122S_040709_1301]
Acknowledgments	Details

- **Contact**: The system contact configured in**Configuration** > **System** > **Information** > **System Contact**.

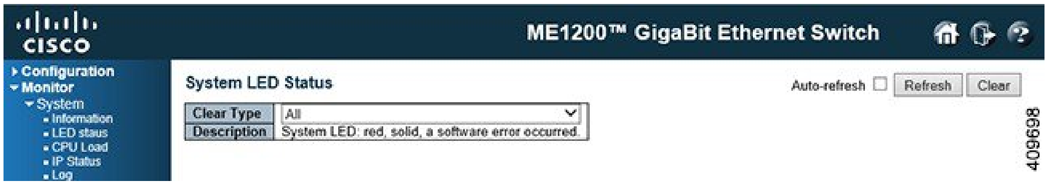
- **Name**: The system name configured in**Configuration** > **System** > **Information** > **System Name**.
- **Location**: The system name configured in**Configuration** > **System** > **Information** > **System Location**.
- **MAC Address**: The MAC Address of this switch.
- **Chip ID**: The Chip ID of this switch.
- **System Date**: The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.
- **System Uptime**: The period of time the device has been operational.
- **Software Version**: The software version of this switch.
- **Software Date**: The date when the switch software was produced.
- **Code Revision**: The version control identifier of the switch software.

Related Topics

Configuring System, on page 21

System LED Status

This option allows you to view the switch system LED status.



System LED Status

Clear Type	All
Description	System LED: red, solid, a software error occurred.

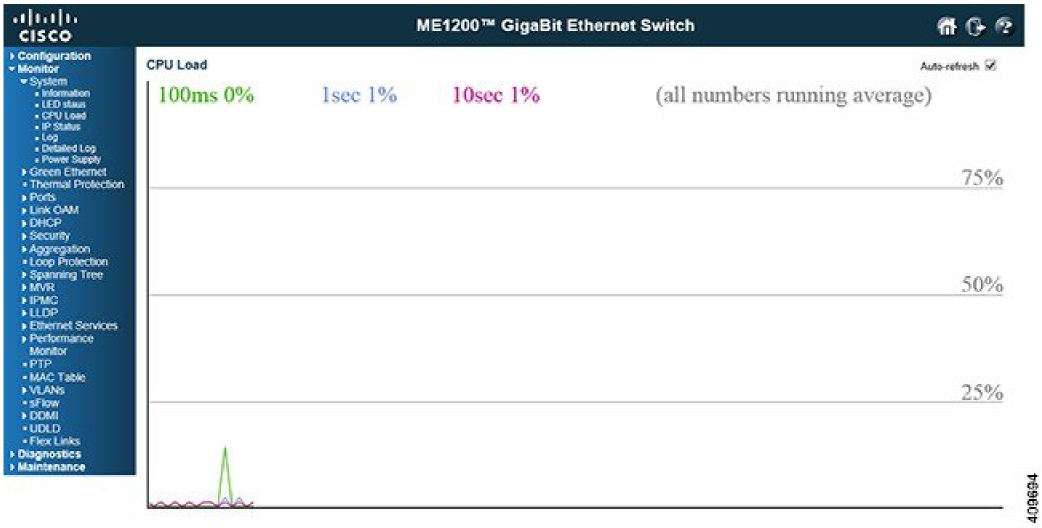
- **Clear Type**: The types of system LED status clearing is listed. Possible values are:
    - *All*: Clear all error status of the system LED and back to normal indication.
    - *Fatal*: Clear fatal error status of the system LED.
    - *Software*: Clear generic software error status of the system LED.
    - *POST*: Clear POST error status of the system LED.
    - *ZTP*: Clear ZTP error status of the system LED.
- **Description**: The description of system LED.

Related Topics

Configuring System, on page 21

CPU Load

This option displays the CPU Load of your system using an SVG graph.



The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well.

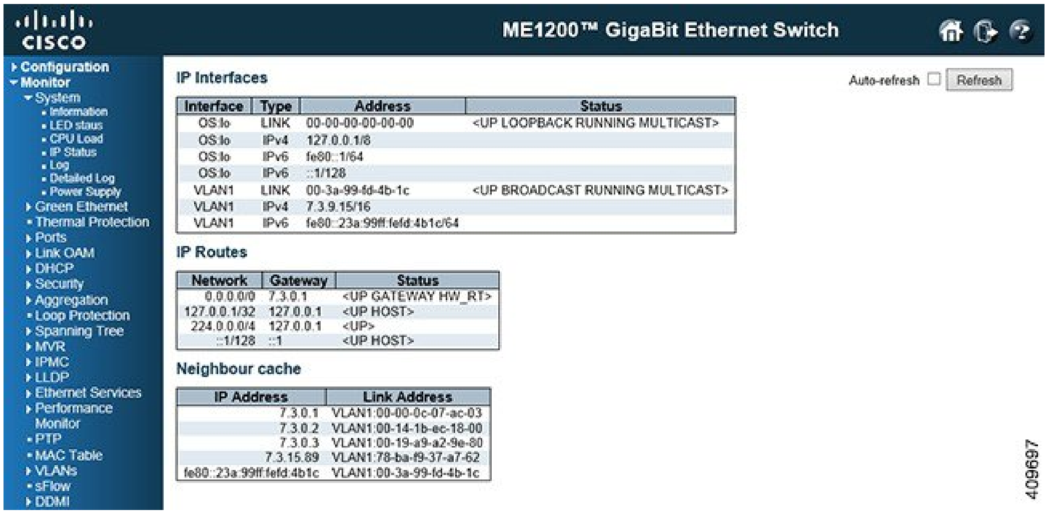
Note In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.

Related Topics

Configuring System, on page 21

IP Status

This option displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbour cache (ARP cache) status.



IP Interfaces

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	fe80::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	00-3a-99-fd-4b-1c	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	7.3.9.15/16	
VLAN1	IPv6	fe80::23a:99ff:fefd:4b1c/64	

IP Routes

Network	Gateway	Status
0.0.0.0/0	7.3.0.1	<UP GATEWAY HW_RT>
127.0.0.1/32	127.0.0.1	<UP HOST>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour cache

IP Address	Link Address
7.3.0.1	VLAN1:00-00-0c-07-ac-03
7.3.0.2	VLAN1:00-14-1b-ec-18-00
7.3.0.3	VLAN1:00-19-a9-a2-9e-80
7.3.15.89	VLAN1:78-ba-f9-37-a7-62
fe80::23a:99ff:fefd:4b1c	VLAN1:00-3a-99-fd-4b-1c

IP Interfaces

The following information on the IP Status of your system is displayed.

Interface	The name of the interface.
Type	The address type of the entry. This may be LINK or IPv4.
Address	The current address of the interface.
Status	The status flags of the interface (and/or address).

Click **Add Interface** to add and configure an IP Interface.

IP Routes

The following information on the IP Routes of your system is displayed.

Network	The destination IP network or host address of this route
Gateway	The gateway address of this route.
Status	The status flags of the route

Click **Add Route** to add and configure an IP Route.

Neighbour cache

The following information of your system's cache is displayed.

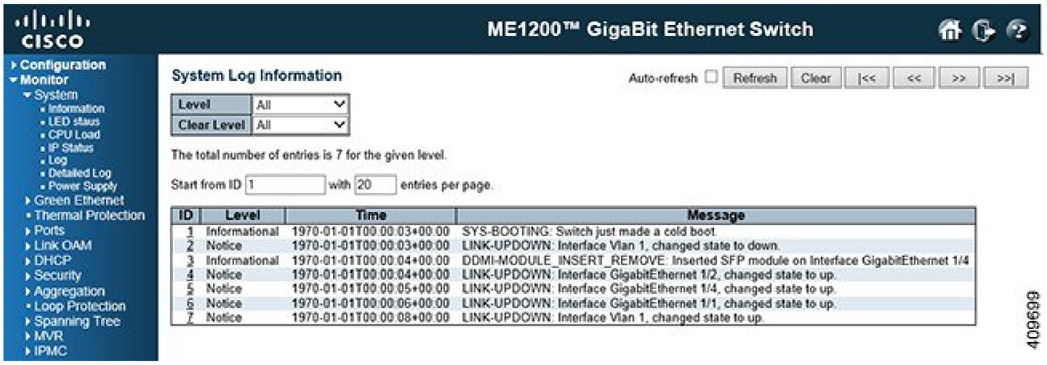
IP Address	The IP address of the entry.
Link Address	The Link(MAC)address for which a binding to the IP address given exist.

Related Topics

Configuring System, on page 21

System Log Information

This option allows you to view the switch system log information.



System Log Information

Level	All
Clear Level	All

The total number of entries is 7 for the given level.

Start from ID 1 with 20 entries per page.

ID	Level	Time	Message
1	Informational	1970-01-01T00:00:03+00:00	SYS-BOOTING: Switch just made a cold boot.
2	Notice	1970-01-01T00:00:03+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
3	Informational	1970-01-01T00:00:04+00:00	DDMI-MODULE_INSERT_REMOVE: Inserted SFP module on Interface GigabitEthernet 1/4
4	Notice	1970-01-01T00:00:04+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/2, changed state to up.
5	Notice	1970-01-01T00:00:05+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/4, changed state to up.
6	Notice	1970-01-01T00:00:06+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/1, changed state to up.
7	Notice	1970-01-01T00:00:08+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.

Navigating the System Log Information Table

Each page shows up to 999 table entries, selected through the **entries per page** input field. When first visited, the web page will show the beginning entries of this table. The **Level** input field is used to filter the display system log entries. The **Clear Level** input field is used to specify which system log entries will be cleared. To clear specific system log entries, select the clear level first then click the **Clear** button.

The **Start from ID** input field allow the user to change the starting point in this table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next entry match. In addition, these input fields will upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

The >> will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text **No more entries** is shown in the displayed table. Use the << button to start over.

System Log Information Entry Columns

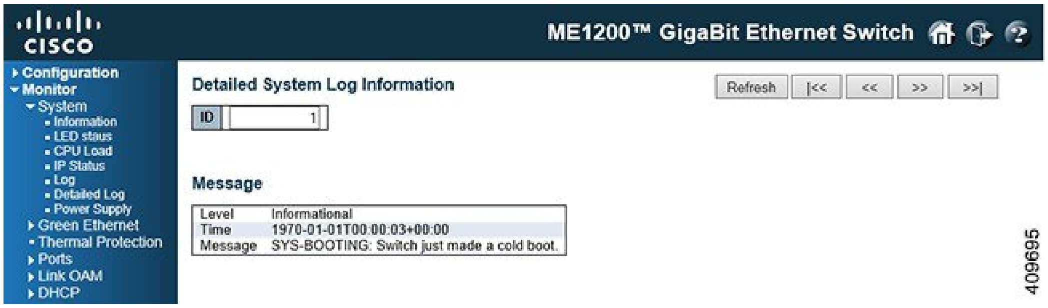
- **ID**: The identification of the system log entry.
- **Level**: The level of the system log entry.
  - **Info**: The system log entry is belonged information level.
  - **Warning**: The system log entry is belonged warning level.
  - **Error**: The system log entry is belonged error level.
- **Time**: The occurred time of the system log entry.
- **Message**: The detail message of the system log entry.

Related Topics

Configuring System, on page 21

Detailed System Log Information

This option displays detailed log information of the switch system.



Detailed System Log Information

ID 1

Message

Level	Informational
Time	1970-01-01T00:00:03+00:00
Message	SYS-BOOTING: Switch just made a cold boot.

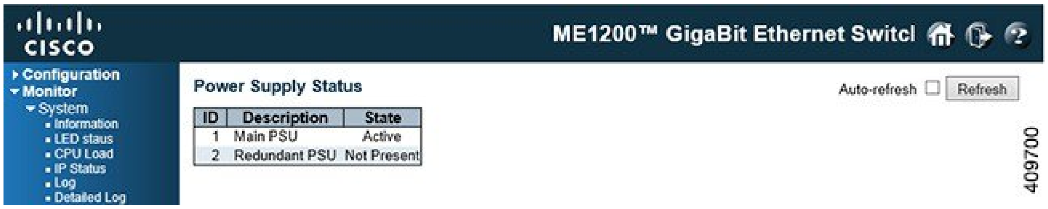
- **Level**: The severity level of the system log entry.
- **ID**: The ID (>= 1) of the system log entry.
- **Message**: The detailed message of the system log entry.

Related Topics

Configuring System, on page 21

System Power Supply Status

This option displays the power supply status of the switch system.



Power Supply Status

ID	Description	State
1	Main PSU	Active
2	Redundant PSU	Not Present

- **ID**: The identification of power supply.
- **Description**: The description of power supply.
- **State**: The description of power supply. Possible values are:
    - **Active**: The power supply is used for the system currently.
    - **Standby**: The power supply is standby as the redundant power supply.
    - **Not Present**: The power supply is not present.

Related Topics

Configuring System, on page 21

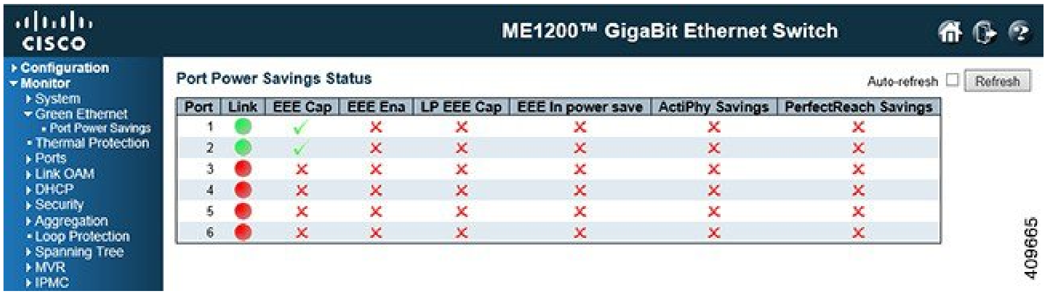
CHAPTER 34

Monitoring Green Ethernet

The Green Ethernet feature available on the ME 1200 Web GUI allows you to monitor the port power savings on the ME 1200 switch.

EEE Status

This option provides the current status for EEE.



Port Power Savings Status

Port	Link	EEE Cap	EEE Ena	LP EEE Cap	EEE In power save	ActiPhy Savings	PerfectReach Savings
1	🟢	✓	✗	✗	✗	✗	✗
2	🟢	✓	✗	✗	✗	✗	✗
3	🔴	✗	✗	✗	✗	✗	✗
4	🔴	✗	✗	✗	✗	✗	✗
5	🔴	✗	✗	✗	✗	✗	✗
6	🔴	✗	✗	✗	✗	✗	✗

- **Local Port**: This is the logical port number for this row.
- **Link**: Shows if the link is up for the port (green = link up, red = link down).
- **EEE cap**: Shows if the port is EEE capable.
- **EEE Ena**: Shows if EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page).
- **LP EEE cap**: Shows if the link partner is EEE capable.
- **EEE In power save**: Shows if the system is currently saving power due to EEE. When EEE is enabled, the system will powered down if no frame has been received or transmitted in 5 microseconds.
- **Actiphy Savings**: Shows if the system is currently saving power due to ActiPhy.
- **PerfectReach Savings**: Shows if the system is currently saving power due to PerfectReach.

Related Topics

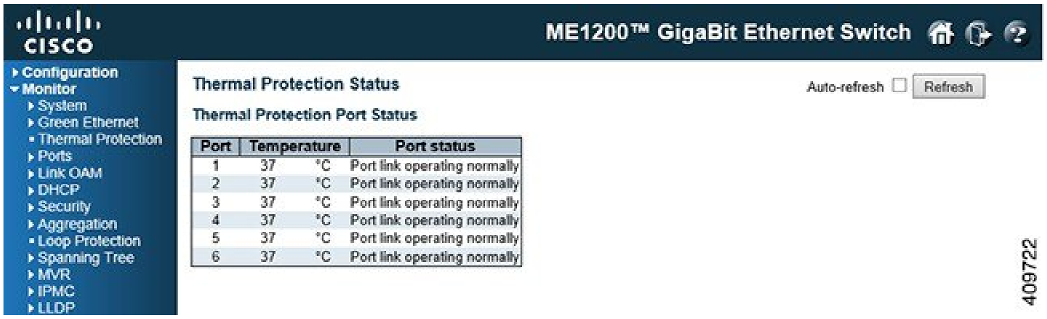
Configuring Green Ethernet, on page 29

CHAPTER 35

Monitoring Thermal Protection

Thermal Protection Status

This option allows the user to inspect status information related to thermal protection.



Thermal Protection Status

Thermal Protection Port Status

Port	Temperature		Port status
1	37	°C	Port link operating normally
2	37	°C	Port link operating normally
3	37	°C	Port link operating normally
4	37	°C	Port link operating normally
5	37	°C	Port link operating normally
6	37	°C	Port link operating normally

- **Port**: The switch port number.
- **Temperature**: Shows the current chip temperature in degrees Celsius.
- **Port Status**: Shows if the port is thermally protected (link is down) or if the port is operating normally.

Related Topics

Configuring Thermal Protection, on page 31

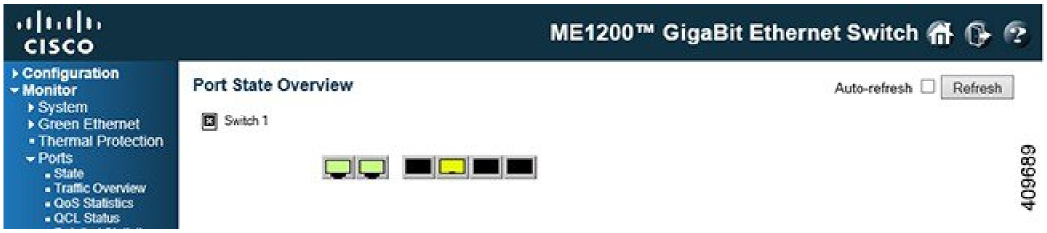
CHAPTER 36

Monitoring Ports

The Ports feature available on the ME 1200 Web GUI allows you to monitor the various port parameters on the ME 1200 switch.

Port State

This option provides an overview of the current switch port states. The port states are illustrated as follows:



Port State Overview

Auto-refresh □ Refresh

☒ Switch 1

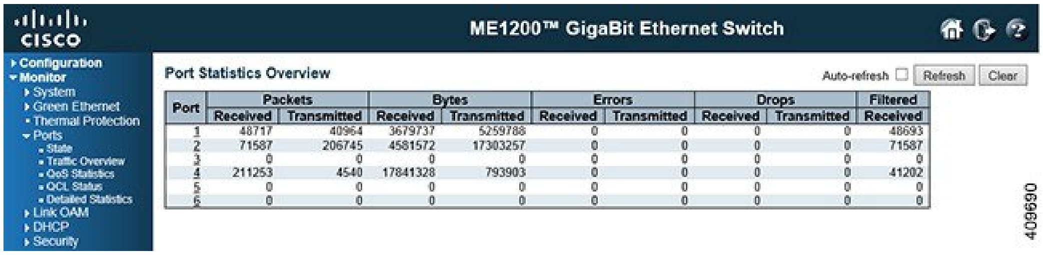
- **RJ45 Ports**
- **SFP Ports**
- **State**
    - ◦ *Disabled*
    - ◦ *Down*
    - ◦ *Link*

Related Topics

Configuring Ports, on page 33

Port Statistics Overview

This option provides an overview of general traffic statistics for all switch ports.



Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	48717	40964	3679737	5259788	0	0	0	0	48693
2	71587	206745	4581572	17303257	0	0	0	0	71587
3	0	0	0	0	0	0	0	0	0
4	211253	4540	17841328	793903	0	0	0	0	41202
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0

The displayed counters are:

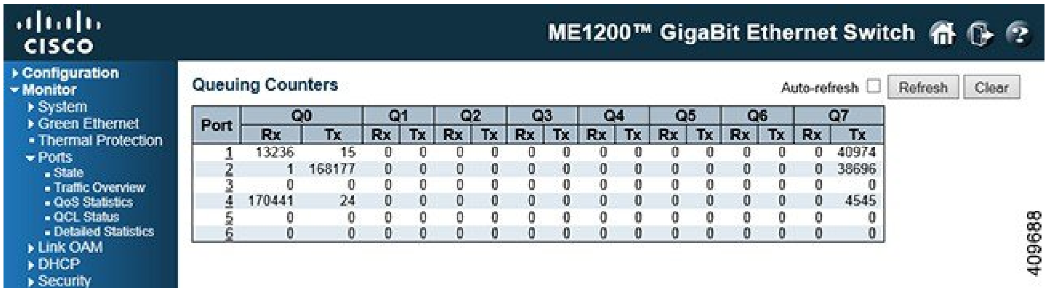
- **Port**: The logical port for the settings contained in the same row.
- **Packets**: The number of received and transmitted packets per port.
- **Bytes**: The number of received and transmitted bytes per port.
- **Errors**: The number of frames received in error and the number of incomplete transmissions per port.
- **Drops**: The number of frames discarded due to ingress or egress congestion.
- **Filtered**: The number of received frames filtered by the forwarding process.

Related Topics

Configuring Ports, on page 33

QoS Statistics

This option provides statistics for the different queues for all switch ports.



Queuing Counters

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	13236	15	0	0	0	0	0	0	0	0	0	0	0	0	0	40974
2	1	168177	0	0	0	0	0	0	0	0	0	0	0	0	0	38696
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	170441	24	0	0	0	0	0	0	0	0	0	0	0	0	0	4545
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

The displayed counters are:

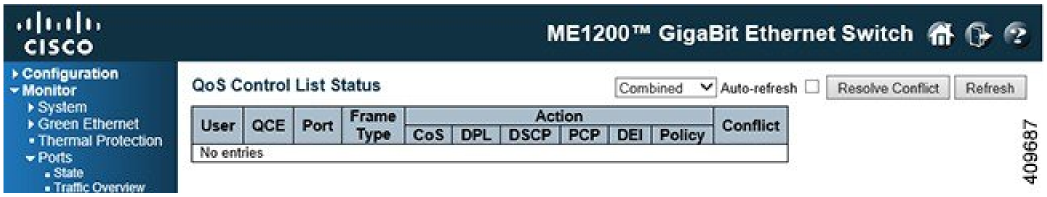
- **Port**: The logical port for the settings contained in the same row.
- **Qn**: There are 8 QoS queues per port. Q0 is the lowest priority queue.
- **Rx/Tx**: The number of received and transmitted packets per queue

Related Topics

Configuring Ports, on page 33

QCL Status

This option shows the QCL status by different QCL users. Each row describes the QCE that is defined.



QoS Control List Status

Combined; Auto-refresh □

User	QCE	Port	Frame Type	Action						Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	
No entries										

It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 1024 on each switch.

- **User**: Indicates the QCL user.
- **QCE**: Indicates the QCE id.
- **Port**: Indicates the list of ports configured with the QCE.
- **Frame Type**: Indicates the type of frame. Possible values are:
  - **Any**: Match any frame type.
  - **Ethernet**: Match EtherType frames.
  - **LLC**: Match (LLC) frames.
  - **SNAP**: Match (SNAP) frames.
  - **IPv4**: Match IPv4 frames.
  - **IPv6**: Match IPv6 frames.
- **Action**: Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are:
  - **CoS**: Classify Class of Service.
  - **DPL**: Classify Drop Precedence Level.
  - **DSCP**: Classify DSCP value.
  - **PCP**: Classify PCP value.
  - **DEI**: Classify DEI value.

- **Policy**: Classify ACL Policy number.

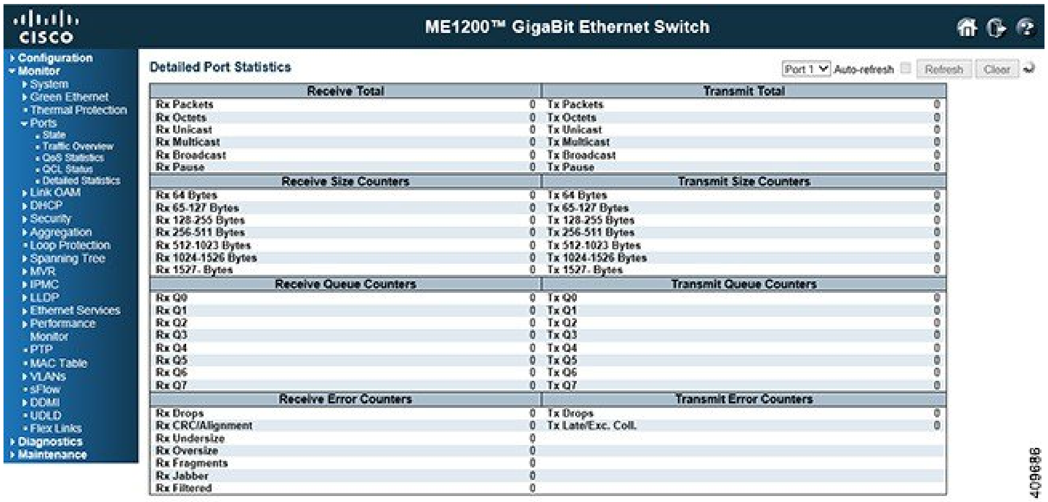
- **Conflict**: Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as ***Yes***, otherwise it is always ***No***. Note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing **Resolve Conflict** button.

Related Topics

Configuring Ports, on page 33

Detailed Port Statistics

This option provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.



Detailed Port Statistics

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	0
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

Receive Total and Transmit Total

- **Rx and Tx Packets**: The number of received and transmitted (good and bad) packets.

- **Rx and Tx Octets**: The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

- **Rx and Tx Unicast**: The number of received and transmitted (good and bad) unicast packets.

- **Rx and Tx Multicast**: The number of received and transmitted (good and bad) multicast packets.

- **Rx and Tx Broadcast**: The number of received and transmitted (good and bad) broadcast packets.

- **Rx and Tx Pause**: A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a **PAUSE** operation.

Receive and Transmit Size Counters

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters

The number of received and transmitted packets per input and output queue.

Receive Error Counters

- **Rx Drops**: The number of frames dropped due to lack of receive buffers or egress congestion.
- **Rx CRC/Alignment**: The number of frames received with CRC or alignment errors.
- **Rx Undersize**: The number of short 1 frames received with valid CRC.
- **Rx Oversize**: The number of long 2 frames received with valid CRC.
- **Rx Fragments**: The number of short 1 frames received with invalid CRC.
- **Rx Jabber**: The number of long 2 frames received with invalid CRC.
- **Rx Filtered**: The number of received frames filtered by the forwarding process.
    - Short frames are frames that are smaller than 64 bytes.
    - Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

- **Tx Drops**: The number of frames dropped due to output buffer congestion.
- Tx **Late/Exc. Coll**: The number of frames dropped due to excessive or late collisions.

Related Topics

Configuring Ports, on page 33

CHAPTER 37

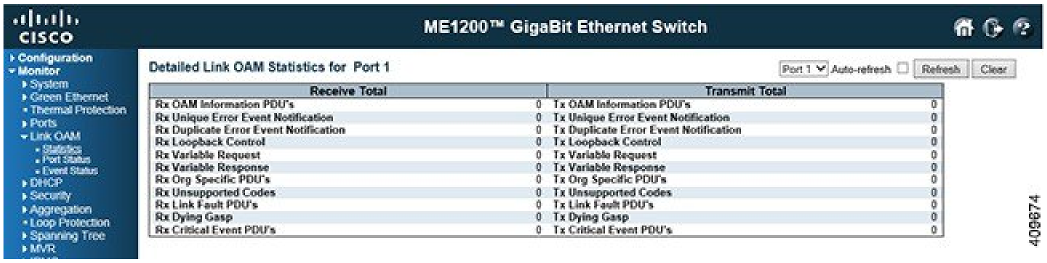
Monitoring Link OAM

The Link OAM feature available on the ME 1200 Web GUI allows you to monitor the Link OAM port and the Link Event for a given port.

Detailed Link OAM Port Statistics

This option provides detailed OAM traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters represent the total number of OAM frames received and transmitted for the selected port. Discontinuities of these counter can occur at re-initialization of the management system.



Detailed Link OAM Statistics for Port 1

Receive Total		Transmit Total	
Rx OAM Information PDU's	0	Tx OAM Information PDU's	0
Rx Unique Error Event Notification	0	Tx Unique Error Event Notification	0
Rx Duplicate Error Event Notification	0	Tx Duplicate Error Event Notification	0
Rx Loopback Control	0	Tx Loopback Control	0
Rx Variable Request	0	Tx Variable Request	0
Rx Variable Response	0	Tx Variable Response	0
Rx Org Specific PDU's	0	Tx Org Specific PDU's	0
Rx Unsupported Codes	0	Tx Unsupported Codes	0
Rx Link Fault PDU's	0	Tx Link Fault PDU's	0
Rx Dying Gasp	0	Tx Dying Gasp	0
Rx Critical Event PDU's	0	Tx Critical Event PDU's	0

Receive Total and Transmit Total

- **Rx and Tx OAM Information PDU's**: The number of received and transmitted OAM Information PDU's. Discontinuities of this counter can occur at re-initialization of the management system.
- **Rx and Tx Unique Error Event Notification**: A count of the number of unique Event OAMPDUs received and transmitted on this interface. Event Notifications may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. Duplicate Event Notification transmissions are counted by Duplicate Event Notification counters for Tx and Rx respectively. A unique Event Notification OAMPDU is indicated as an Event Notification

OAMPDU with a Sequence Number field that is distinct from the previously transmitted Event Notification OAMPDU Sequence Number.

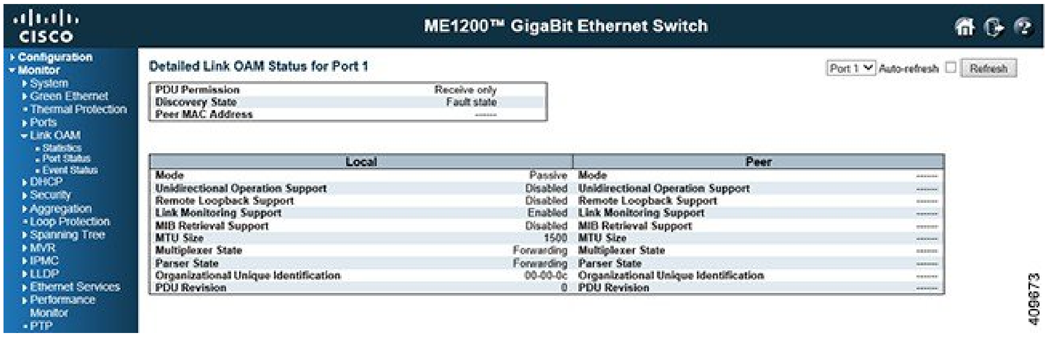
- **Rx and Tx Duplicate Error Event Notification**: A count of the number of duplicate Event OAMPDUs received and transmitted on this interface. Event Notification OAMPDUs may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. A duplicate Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is identical to the previously transmitted Event Notification OAMPDU Sequence Number.
- **Rx and Tx Loopback Control**: A count of the number of Loopback Control OAMPDUs received and transmitted on this interface.
- **Rx and Tx Variable Request**: A count of the number of Variable Request OAMPDUs received and transmitted on this interface.
- **Rx and Tx Variable Response**: A count of the number of Variable Response OAMPDUs received and transmitted on this interface.
- **Rx and Tx Org Specific PDU's**: A count of the number of Organization Specific OAMPDUs transmitted on this interface.
- **Rx and Tx Unsupported Codes**: A count of the number of OAMPDUs transmitted on this interface with an unsupported op-code.
- **Rx and Tx Link fault PDU's**: A count of the number of Link fault PDU's received and transmitted on this interface.
- **Rx and Tx Dying Gasp**: A count of the number of Dying Gasp events received and transmitted on this interface.
- **Rx and Tx Critical Event PDU's**: A count of the number of Critical event PDU's received and transmitted on this interface.

Related Topics

Configuring Link OAM, on page 59

Link OAM Port Configuration Status

This option provides Link OAM configuration operational status. The displayed fields shows the active configuration status for the selected port.



Detailed Link OAM Status for Port 1

PDU Permission	Receive only
Discovery State	Fault state
Peer MAC Address	-------

Local		Peer	
Mode	Passive	Mode	-------
Unidirectional Operation Support	Disabled	Unidirectional Operation Support	-------
Remote Loopback Support	Disabled	Remote Loopback Support	-------
Link Monitoring Support	Enabled	Link Monitoring Support	-------
MIB Retrieval Support	Disabled	MIB Retrieval Support	-------
MTU Size	1500	MTU Size	-------
Multiplexer State	Forwarding	Multiplexer State	-------
Parser State	Forwarding	Parser State	-------
Organizational Unique Identification	00-00-0c	Organizational Unique Identification	-------
PDU Revision	0	PDU Revision	-------

Local and Peer

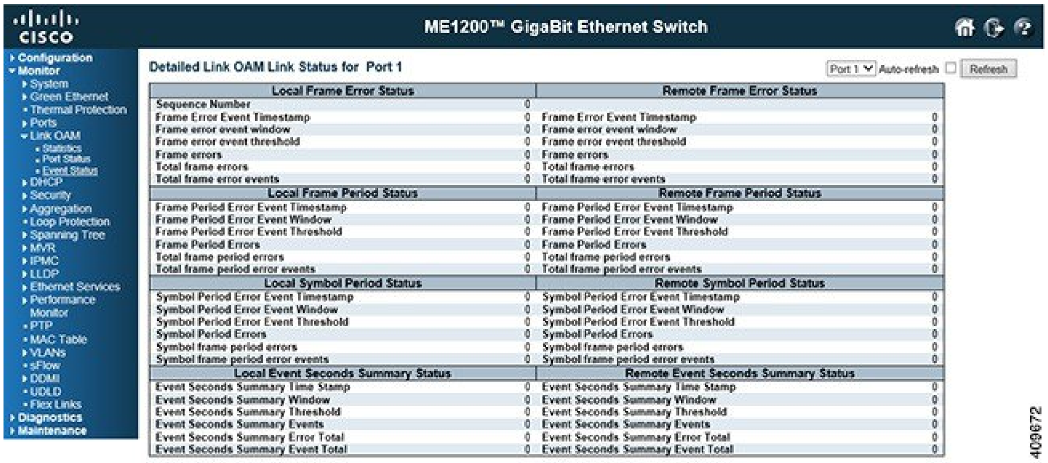
- **Mode**: The Mode in which the Link OAM is operating, *Active* or *Passive*.
- **Unidirectional Operation Support**: This feature is not available to be configured by the user. The status of this configuration is retrieved from the PHY.
- **Remote Loopback Support**: If status is enabled, DTE is capable of OAM remote loopback mode.
- **Link Monitoring Support**: If status is enabled, DTE supports interpreting Link Events.
- **MIB Retrieval Support**: If status ie enabled DTE supports sending Variable Response OAMPDUs.
- **MTU Size**: It represents the largest OAMPDU, in octets, supported by the DTE. This value is compared to the remotes Maximum PDU Size and the smaller of the two is used.
- **Multiplexer State**: When in forwarding state, the Device is forwarding non-OAMPDUs to the lower sublayer. Incase of discarding, the device discards all the non-OAMPDU's.
- **Parser State**: When in forwarding state, Device is forwarding non-OAMPDUs to higher sublayer. When in loopback, Device is looping back non-OAMPDUs to the lower sublayer. When in discarding state, Device is discarding non-OAMPDUs.
- **Organizational Unique Identification**: 24-bit Organizationally Unique Identifier of the vendor.
- **PDU Revision**: It indicates the current revision of the Information TLV. The value of this field shall start at zero and be incremented each time something in the Information TLV changes. Upon reception of an Information TLV from a peer, an OAM client may use this field to decide if it needs to be processed (an Information TLV that is identical to the previous Information TLV does not need to be parsed as nothing in it has changed).
- **PDU Permission**: This field is available only for the Local DTE. It displays the current permission rules set for the local DTE. Possible values are *Link fault*,*Receive only*, *Information exchange only*, *ANY*.
- **Discovery State**: Displays the current state of the discovery process. Possible states are *Fault state*, *Active state*, *Passive state*, *SEND_LOCAL_REMOTE_STATE*, *SEND_LOCAL_REMOTE_OK_STATE*, *SEND_ANY_STATE*.

Related Topics

Configuring Link OAM, on page 59

Link OAM Link Event Status

This option allows the user to inspect the current Link OAM Link Event configurations, and change them as well. The left pane displays the Event status for the Local OAM unit while the right pane displays the status for the Peer for the respective port.



Detailed Link OAM Link Status for Port 1

Local Frame Error Status		Remote Frame Error Status	
Sequence Number	0		
Frame Error Event Timestamp	0	Frame Error Event Timestamp	0
Frame error event window	0	Frame error event window	0
Frame error event threshold	0	Frame error event threshold	0
Frame errors	0	Frame errors	0
Total frame errors	0	Total frame errors	0
Total frame error events	0	Total frame error events	0
Local Frame Period Status		**Remote Frame Period Status**	
Frame Period Error Event Timestamp	0	Frame Period Error Event Timestamp	0
Frame Period Error Event Window	0	Frame Period Error Event Window	0
Frame Period Error Event Threshold	0	Frame Period Error Event Threshold	0
Frame Period Errors	0	Frame Period Errors	0
Total frame period errors	0	Total frame period errors	0
Total frame period error events	0	Total frame period error events	0
Local Symbol Period Status		**Remote Symbol Period Status**	
Symbol Period Error Event Timestamp	0	Symbol Period Error Event Timestamp	0
Symbol Period Error Event Window	0	Symbol Period Error Event Window	0
Symbol Period Error Event Threshold	0	Symbol Period Error Event Threshold	0
Symbol Period Errors	0	Symbol Period Errors	0
Symbol frame period errors	0	Symbol frame period errors	0
Symbol frame period error events	0	Symbol frame period error events	0
Local Event Seconds Summary Status		**Remote Event Seconds Summary Status**	
Event Seconds Summary Time Stamp	0	Event Seconds Summary Time Stamp	0
Event Seconds Summary Window	0	Event Seconds Summary Window	0
Event Seconds Summary Threshold	0	Event Seconds Summary Threshold	0
Event Seconds Summary Events	0	Event Seconds Summary Events	0
Event Seconds Summary Error Total	0	Event Seconds Summary Error Total	0
Event Seconds Summary Event Total	0	Event Seconds Summary Event Total	0

- **Port**: The switch port number.
- **Sequence Number**: This two-octet field indicates the total number of events occurred at the remote end.
- **Frame Error Event Timestamp**: This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.
- **Frame error event window**: This two-octet field indicates the duration of the period in terms of 100 ms intervals.

  1. The default value is one second.
  2. The lower bound is one second.
  3. The upper bound is one minute.

- **Frame error event threshold**: This four-octet field indicates the number of detected errored frames in the period is required to be equal to or greater than in order for the event to be generated.

  1. The default value is one frame error.
  2. The lower bound is zero frame errors.
  3. The upper bound is unspecified.

- **Frame errors**: This four-octet field indicates the number of detected errored frames in the period.
- **Total frame errors**: This eight-octet field indicates the sum of errored frames that have been detected since the OAM sublayer was reset.
- **Total frame error events**: This four-octet field indicates the number of Errored Frame Event TLVs that have been generated since the OAM sublayer was reset.
- **Frame Period Error Event Timestamp**: This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.
- **Frame Period Error Event Window**: This four-octet field indicates the duration of period in terms of frames.

- **Frame Period Error Event Threshold**: This four-octet field indicates the number of errored frames in the period is required to be equal to or greater than in order for the event to be generated.
- **Frame Period Errors**: This four-octet field indicates the number of frame errors in the period.
- **Total frame period error events**: This four-octet field indicates the number of Errored Frame Period Event TLVs that have been generated since the OAM sublayer was reset.
- **Symbol Period Error Event Timestamp**: This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.
- **Symbol Period Error Event Window**: This eight-octet field indicates the number of symbols in the period.
- **Symbol Period Error Event Threshold**: This eight-octet field indicates the number of errored symbols in the period is required to be equal to or greater than in order for the event to be generated.
- **Symbol Period Errors**: This eight-octet field indicates the number of symbol errors in the period.
- **Symbol frame period errors**: This eight-octet field indicates the sum of symbol errors since the OAM sublayer was reset.
- **Symbol frame period error events**: This four-octet field indicates the number of Errored Symbol Period Event TLVs that have been generated since the OAM sublayer was reset.
- **Event Seconds Summary Time Stamp**: This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.
- **Event Seconds Summary Window**: This two-octet field indicates the duration of the period in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.
- **Event Seconds Summary Threshold**: This two-octet field indicates the number of errored frame seconds in the period is required to be equal to or greater than in order for the event to be generated, encoded as a 16-bit unsigned integer.
- **Event Seconds Summary Events**: This two-octet field indicates the number of errored frame seconds in the period, encoded as a 16-bit unsigned integer.
- **Event Seconds Summary Error Total**: This four-octet field indicates the sum of errored frame seconds that have been detected since the OAM sublayer was reset.
- **Event Seconds Summary Event Total**: This four-octet field indicates the number of Errored Frame Seconds Summary Event TLVs that have been generated since the OAM sublayer was reset, encoded as a 32bit unsigned integer.

Related Topics

Configuring Link OAM, on page 59

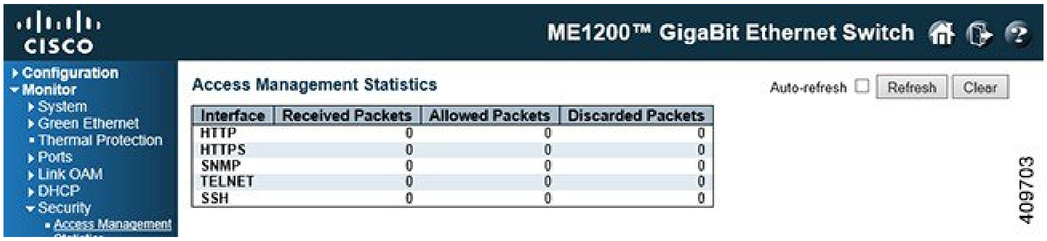
CHAPTER 38

Monitoring Security

The Security feature available on the ME 1200 Web GUI allows you to monitor the security configurations set for the ME 1200 switch.

Access Management Statistics

This option provides statistics for access management as shown below:



Access Management Statistics

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

Interface	The interface type through which the remote host can access the switch.
Received Packets	Number of received packets from the interface when access management mode is enabled.
Allowed Packets	Number of allowed packets from the interface when access management mode is enabled.
Discarded Packets	Number of discarded packets from the interface when access management mode is enabled.

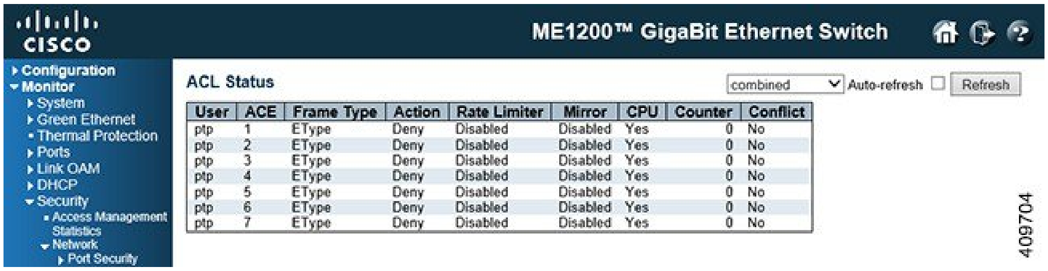
Related Topics

Configuring Security, on page 35

Network

ACL Status

This option shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 512 on each switch.



ACL Status

combined Auto-refresh □ Refresh

User	ACE	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	Conflict
ptp	1	EType	Deny	Disabled	Disabled	Yes	0	No
ptp	2	EType	Deny	Disabled	Disabled	Yes	0	No
ptp	3	EType	Deny	Disabled	Disabled	Yes	0	No
ptp	4	EType	Deny	Disabled	Disabled	Yes	0	No
ptp	5	EType	Deny	Disabled	Disabled	Yes	0	No
ptp	6	EType	Deny	Disabled	Disabled	Yes	0	No
ptp	7	EType	Deny	Disabled	Disabled	Yes	0	No

- **User**: Indicates the ACL user.
- **ACE**: Indicates the ACE ID on local switch.
- **Frame Type**: Indicates the frame type of the ACE. Possible values are:
    - *Any*: The ACE will match any frame type.
    - *EType*: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.
    - *ARP*: The ACE will match ARP/RARP frames.
    - *IPv4*: The ACE will match all IPv4 frames.
    - *IPv4/ICMP*: The ACE will match IPv4 frames with ICMP protocol.
    - *IPv4/UDP*: The ACE will match IPv4 frames with UDP protocol.
    - *IPv4/TCP*: The ACE will match IPv4 frames with TCP protocol.
    - *IPv4/Other*: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
    - *IPv6*: The ACE will match all IPv6 standard frames.
- **Action**: Indicates the forwarding action of the ACE.
    - *Permit*: Frames matching the ACE may be forwarded and learned.
    - *Deny*: Frames matching the ACE are dropped.
    - *Filter*: Frames matching the ACE are filtered.

- **Rate Limiter**: Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
- **CPU**: Forward packet that matched the specific ACE to CPU.
- **Counter**: The counter indicates the number of times the ACE was hit by a frame.
- **Conflict**: Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Related Topics

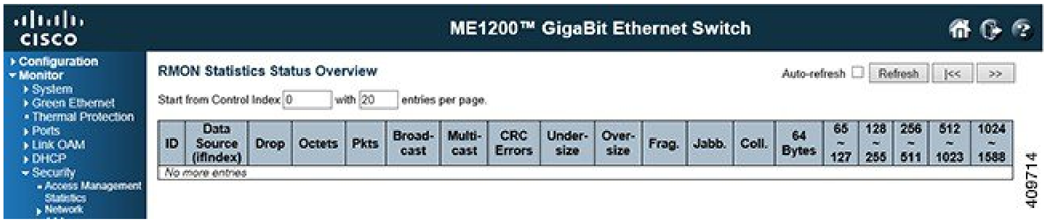
Configuring Security, on page 35

Switch

RMON

RMON Statistics Overview

This option provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the **entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.



RMON Statistics Status Overview

Start from Control Index 0 with 20 entries per page.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
No more entries																		

The **Start from Control Index** allows the user to select the starting point in the Statistics table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Statistics table match.

The >> will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text **No more entries** is shown in the displayed table. Use the **|<<** button to start over.

The displayed counters are:

- **ID**: Indicates the index of Statistics entry.
- **Data Source(ifIndex)**: The port ID which wants to be monitored.
- **Drop**: The total number of events in which packets were dropped by the probe due to lack of resources.
- **Octets**: The total number of octets of data (including those in bad packets) received on the network.
- **Pkts**: The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

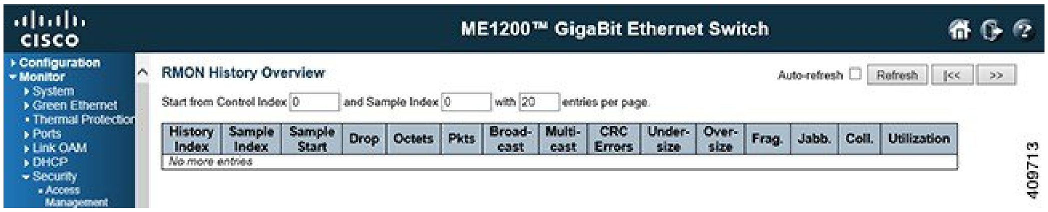
- **Broad-cast**: The total number of good packets received that were directed to the broadcast address.
- **Multi-cast**: The total number of good packets received that were directed to a multicast address.
- **CRC Errors**: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non integral number of octets (Alignment Error).
- **Under-size**: The total number of packets received that were less than 64 octets.
- **Over-size**: The total number of packets received that were longer than 1518 octets.
- **Frag.**: The number of frames which size is less than 64 octets received with invalid CRC.
- **Jabb.**: The number of frames which size is larger than 64 octets received with invalid CRC.
- **Coll.**: The best estimate of the total number of collisions on this Ethernet segment.
- **64**: The total number of packets (including bad packets) received that were 64 octets in length.
- **65~127**: The total number of packets (including bad packets) received that were between 65 to 127 octets in length.
- **128~255**: The total number of packets (including bad packets) received that were between 128 to 255 octets in length.
- **256~511**: The total number of packets (including bad packets) received that were between 256 to 511 octets in length.
- **512~1023**: The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.
- **1024~1588**: The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

Related Topics

Configuring Security, on page 35

RMON History Overview

This option provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the **entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.



RMON History Overview

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
No more entries														

The **Start from History Index and Sample Index** allows the user to select the starting point in the History table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest History table match.

The >> will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text **No more entries** is shown in the displayed table. Use the |<< button to start over.

The displayed fields are:

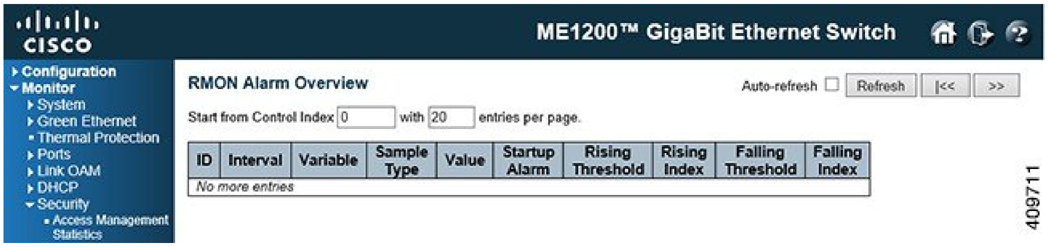
- **History Index**: Indicates the index of History control entry.
- **Sample Index**: Indicates the index of the data entry associated with the control entry.
- **Sample Start**: The value of sysUpTime at the start of the interval over which this sample was measured.
- **Drop**: The total number of events in which packets were dropped by the probe due to lack of resources.
- **Octets**: The total number of octets of data (including those in bad packets) received on the network.
- **Pkts**: The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
- **Broadcast**: The total number of good packets received that were directed to the broadcast address.
- **Multicast**: The total number of good packets received that were directed to a multicast address.
- **CRCErrors**: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
- **Undersize**: The total number of packets received that were less than 64 octets.
- **Oversize**: The total number of packets received that were longer than 1518 octets.
- **Frag.**: The number of frames which size is less than 64 octets received with invalid CRC.
- **Jabb.**: The number of frames which size is larger than 64 octets received with invalid CRC.
- **Coll.**: The best estimate of the total number of collisions on this Ethernet segment.
- **Utilization**: The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Related Topics

Configuring Security, on page 35

RMON Alarm Overview

This option provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the **entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.



RMON Alarm Overview

Auto-refresh □ Refresh |<< >>

Start from Control Index 0 with 20 entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No more entries									

The **Start from Control Index** allows the user to select the starting point in the Alarm table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Alarm table match.

The >> will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text **No more entries** is shown in the displayed table. Use the **|<<** button to start over.

The displayed fields are:

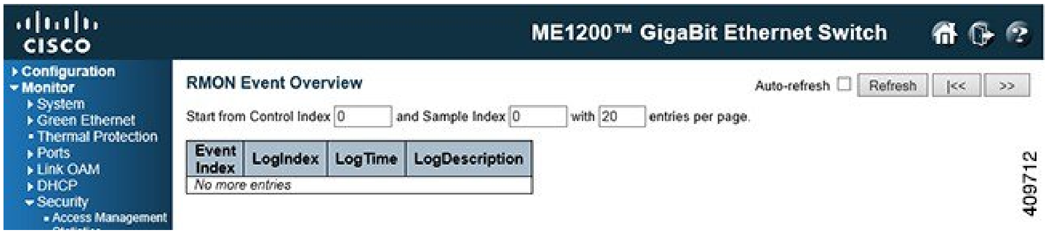
- **ID**: Indicates the index of Alarm control entry.
- **Interval**: Indicates the interval in seconds for sampling and comparing the rising and falling threshold.
- **Variable**: Indicates the particular variable to be sampled.
- **Sample Type**: The method of sampling the selected variable and calculating the value to be compared against the thresholds.
- **Value**: The value of the statistic during the last sampling period.
- **Startup Alarm**: The alarm that may be sent when this entry is first set to valid.
- **Rising Threshold**: Rising threshold value.
- **Rising Index**: Rising event index.
- **Falling Threshold**: Falling threshold value.
- **Falling Index**: Falling event index.

Related Topics

Configuring Security, on page 35

RMON Event Overview

This option provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the **entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table.



RMON Event Overview

Auto-refresh □ Refresh |<< >>

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

Event Index	LogIndex	LogTime	LogDescription
No more entries			

The **Start from Event Index and Log Index** allows the user to select the starting point in the Event table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Event table match.

The >> will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text **No more entries** is shown in the displayed table. Use the **|<<** button to start over.

- **Event Index**: Indicates the index of the event entry.
- **Log Index**: Indicates the index of the log entry.
- Log**Time**: Indicates Event log time.
- **LogDescription**: Indicates the Event description.

Related Topics

Configuring Security, on page 35

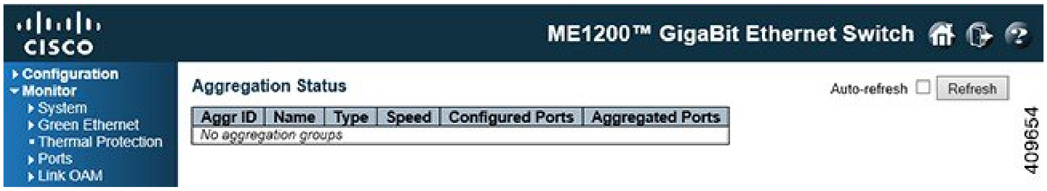
CHAPTER 39

Monitoring Aggregation

The Aggregation feature available on the ME 1200 Web GUI allows you to monitor the Aggregation Mode, Aggregation Group, and LACP port on the ME 1200 switch.

Aggregation Status

This option is used to see the staus of ports in Aggregation group.



Aggregation Status

Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports
No aggregation groups					

Aggregation Group Status

- **Aggr ID**: The Aggregation ID associated with this aggregation instance.
- **Name**: Name of the Aggregation group ID.
- **Type**: Type of the Aggregation group(Static or LACP).
- **Speed**: Speed of the Aggregation group.
- **Configured ports**: Configured member ports of the Aggregation group.
- **Aggregated ports**: Aggregated member ports of the Aggregation group.

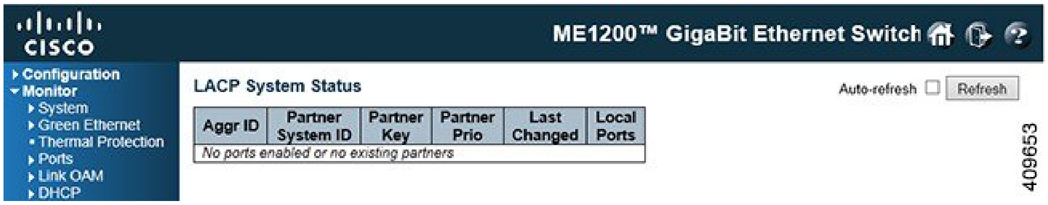
Related Topics

Configuring Aggregation, on page 55

LACP

LACP System Status

This option provides a status overview for all LACP instances.



LACP System Status

Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
No ports enabled or no existing partners					

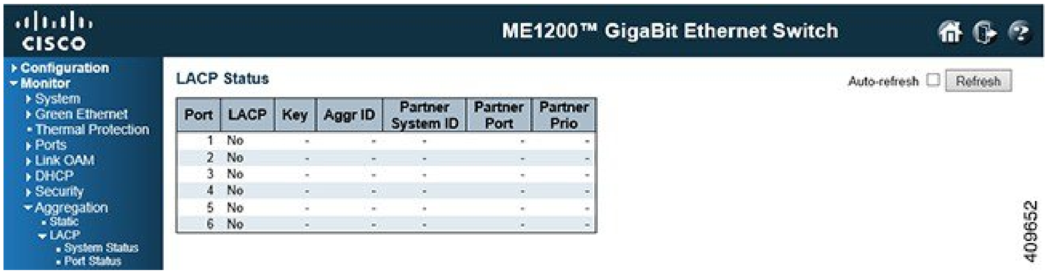
- **Aggr ID**: The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as *isid:aggr-id* and for GLAGs as *aggr-id*.
- **Partner System ID**: The system ID (MAC address) of the aggregation partner.
- **Partner Key**: The Key that the partner has assigned to this aggregation ID.
- **Last changed**: The time since this aggregation changed.
- **Local Ports**: Shows which ports are a part of this aggregation for this switch.

Related Topics

Configuring Aggregation, on page 55

LACP Port Status

This option provides a status overview for LACP status for all ports.



LACP Status

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-

- **Port**: The switch port number.
- **LACP**: *Yes* means that LACP is enabled and the port link is up. *No* means that LACP is not enabled or that the port link is down. *Backup* means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.

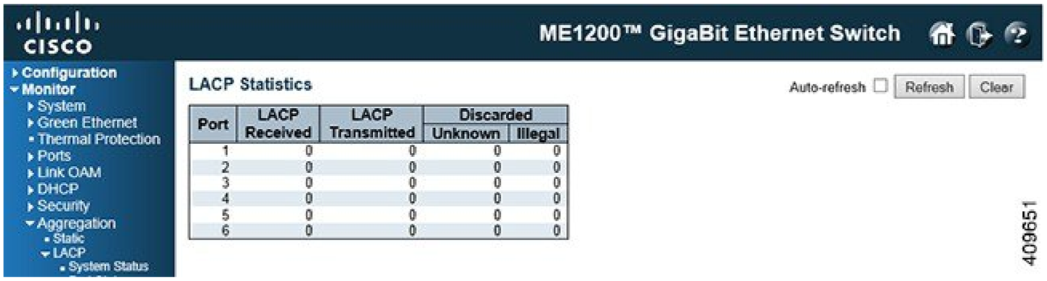
- **Key**: The key assigned to this port. Only ports with the same key can aggregate together.
- **Aggr ID**: The Aggregation ID assigned to this aggregation group.
- **Partner System ID**: The partner's System ID (MAC address).
- **Partner Port**: The partner's port number connected to this port.
- **Partner Prio**: The partner's port priority.

Related Topics

Configuring Aggregation, on page 55

LACP Statistics

This option provides an overview for LACP statistics for all ports.



LACP Statistics

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0

- **Port**: The switch port number.
- **LACP Received**: Shows how many LACP frames have been received at each port.
- **LACP Transmitted**: Shows how many LACP frames have been sent from each port.
- **Discarded**: Shows how many unknown or illegal LACP frames have been discarded at each port.

Related Topics

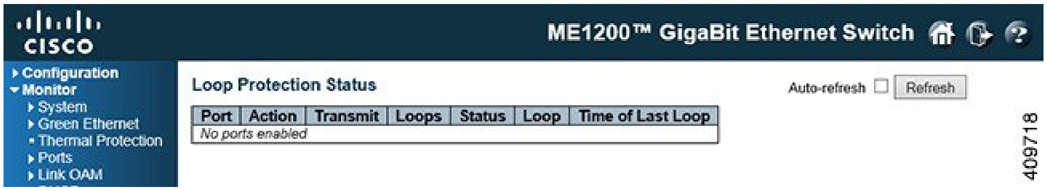
Configuring Aggregation, on page 55

CHAPTER 40

Monitoring Loop Protection

Loop Protection Status

This option displays the loop protection port status the ports of the switch.



Loop Protection Status

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
No ports enabled						

- **Port**: The switch port number of the logical port.
- **Action**: The currently configured port action.
- **Transmit**: The currently configured port transmit mode.
- **Loops**: The number of loops detected on this port.
- **Status**: The current loop protection status of the port.
- **Loop**: Whether a loop is currently detected on the port.
- **Time of Last Loop**: The time of the last loop event detected.

Related Topics

Configuring Loop Protection, on page 63

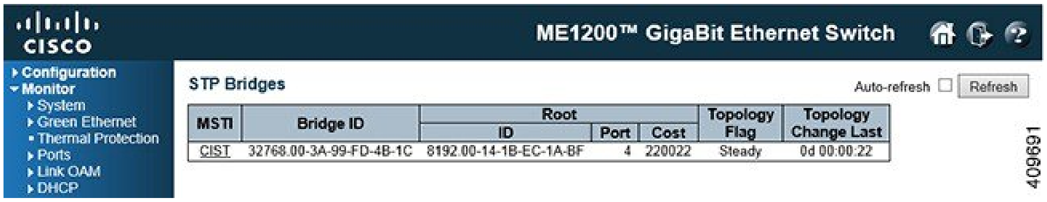
CHAPTER 41

Monitoring Spanning Tree

The Spanning Tree feature available on the ME 1200 Web GUI allows you to monitor the Bridge, MSTI, and CIST settings on the ME 1200 switch.

STP Bridge Status

This option provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance, where the column displays the following information:



STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-3A-99-FD-4B-1C	8192.00-14-1B-EC-1A-BF	4	220022	Steady	0d 00:00:22

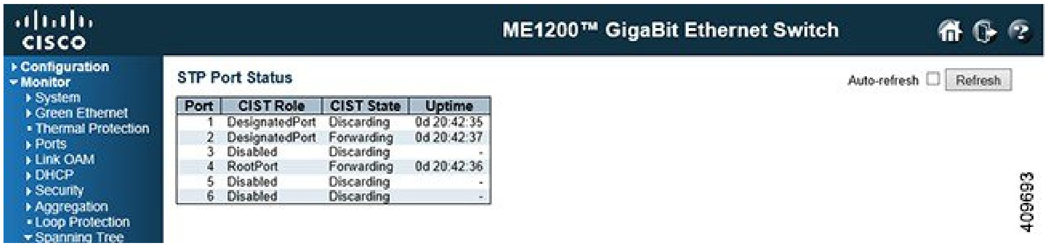
- **MSTI**: The Bridge Instance. This is also a link to the STP Detailed Bridge Status.
- **Bridge ID**: The Bridge ID of this Bridge instance.
- **Root ID**: The Bridge ID of the currently elected root bridge.
- **Root Port**: The switch port currently assigned the root port role.
- **Root Cost**: Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
- **Topology Flag**: The current state of the Topology Change Flag of this Bridge instance.
- **Topology Change Last**: The time since last Topology Change occurred.

Related Topics

Configuring Spanning Tree, on page 65

STP Port Status

This option displays the STP CIST port status for physical ports of the switch.



STP Port Status

Port	CIST Role	CIST State	Uptime
1	DesignatedPort	Discarding	0d 20:42:35
2	DesignatedPort	Forwarding	0d 20:42:37
3	Disabled	Discarding	-
4	RootPort	Forwarding	0d 20:42:36
5	Disabled	Discarding	-
6	Disabled	Discarding	-

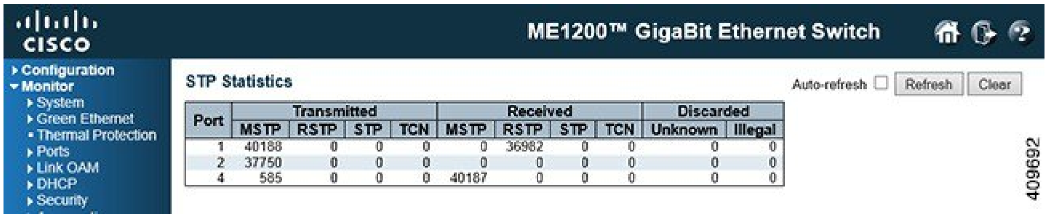
- **Port**: The switch port number of the logical STP port.
- **CIST Role**: The current STP port role of the CIST port. The port role can be one of the following values: *AlternatePort*, *BackupPort*, *RootPort*, *DesignatedPort*, *Disabled*.
- **CIST State**: The current STP port state of the CIST port. The port state can be one of the following values: *Discarding*, *Learning*, *Forwarding*.
- **Uptime**: The time since the bridge port was last initialized.

Related Topics

Configuring Spanning Tree, on page 65

STP Port Statistics

This option displays the STP port statistics counters of bridge ports in the switch. The STP port statistics counters are:



STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	40188	0	0	0	0	36982	0	0	0	0
2	37750	0	0	0	0	0	0	0	0	0
4	585	0	0	0	40187	0	0	0	0	0

- **Port**: The switch port number of the logical STP port.
- **MSTP**: The number of MSTP BPDU's received/transmitted on the port.
- **RSTP**: The number of RSTP BPDU's received/transmitted on the port.
- **STP**: The number of legacy STP Configuration BPDU's received/transmitted on the port.

- **TCN**: The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.
- **Discarded Unknown**: The number of unknown Spanning Tree BPDU's received (and discarded) on the port.
- **Discarded Illegal**: The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Related Topics

Configuring Spanning Tree, on page 65

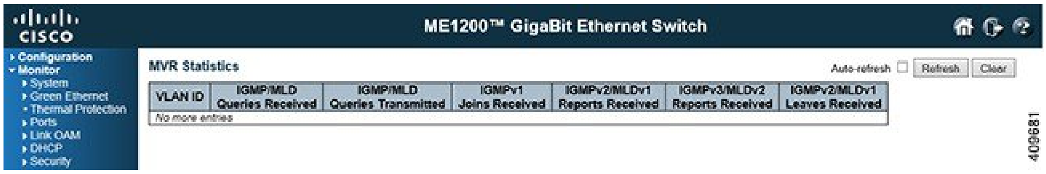
CHAPTER 42

Monitoring MVR

The MVR feature available on the ME 1200 Web GUI allows you to monitor the MVR Channels and view the MVR SFM Information Table.

MVR Statistics Table

This option provides MVR Statistics information.



MVR Statistics

VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
No more entries						

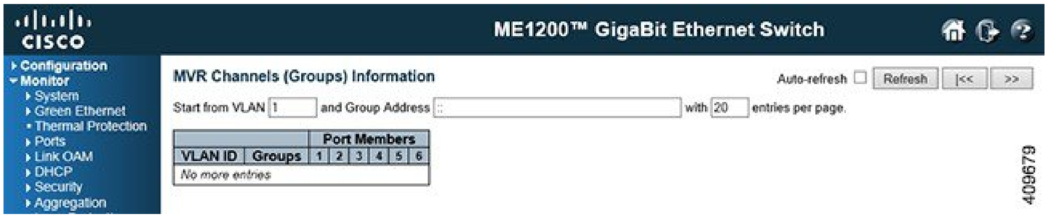
- **VLAN ID**: The Multicast VLAN ID.
- **IGMP/MLD Queries Received**: The number of Received Queries for IGMP and MLD, respectively.
- **IGMP/MLD Queries Transmitted**: The number of Transmitted Queries for IGMP and MLD, respectively.
- **IGMPv1 Joins Received**: The number of Received IGMPv1 Join's.
- **IGMPv2/MLDv1 Report's Received**: The number of Received IGMPv2 Join's and MLDv1 Report's, respectively.
- **IGMPv3/MLDv2 Report's Received**: The number of Received IGMPv1 Join's and MLDv2 Report's, respectively.
- **IGMPv2/MLDv1 Leave's Received**: The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively.

Related Topics

Configuring MVR, on page 71

MVR Channels (Groups) Information Table

This option displays the entries in the MVR Channels (Groups) Information Table.



MVR Channels (Groups) Information

Auto-refresh □ Refresh |<< >>

Start from VLAN 1 and Group Address :: with 20 entries per page.

		Port Members					
VLAN ID	Groups	1	2	3	4	5	6
No more entries							

The MVR Channels (Groups) Information Table is sorted first by VLAN ID, and then by group.

Navigating the MVR Channels (Groups) Information Table

Each page shows up to 99 entries from the MVR Group table, default being 20, selected through the **entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR Channels (Groups) Information Table.

The **Start from VLAN**, and **Group Address** input fields allow the user to select the starting point in the MVR Channels (Groups) Information Table.

Clicking the **Refresh** button will update the displayed table starting from that or the closest next MVR Channels (Groups) Information Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The >> will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text **No more entries** is shown in the displayed table. Use the **|<<** button to start over.

MVR Channels (Groups) Information Table Columns

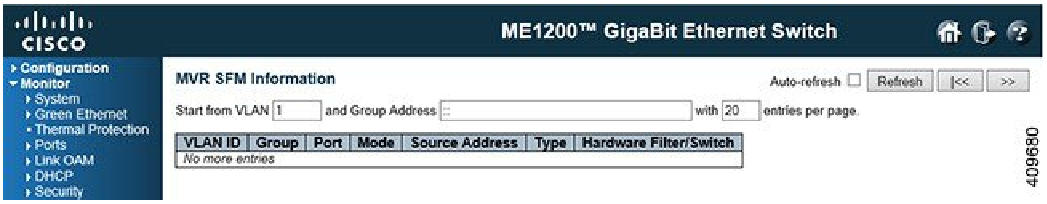
- **VLAN ID**: VLAN ID of the group.
- **Groups**: Group ID of the group displayed.
- **Port Members**: Ports under this group.

Related Topics

Configuring MVR, on page 71

MVR SFM Information Table

This option displays the entries in the MVR SFM Information Table.



MVR SFM Information

Start from VLAN 1 and Group Address :: with 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Navigating the MVR SFM Information Table

Each page shows up to 99 entries from the MVR SFM Information Table, default being 20, selected through the **entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR SFM Information Table.

The **Start from VLAN**, and **Group Address** input fields allow the user to select the starting point in the MVR SFM Information Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next MVR SFM Information Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text **No more entries** is shown in the displayed table. Use the |<< button to start over.

MVR SFM Information Table Columns

- **VLAN ID**: VLAN ID of the group.
- **Group**: Group address of the group displayed.
- **Port**: Switch port number.
- **Mode**: Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either *Include* or *Exclude*.
- **Source Address**: IP Address of the source.

  Currently, the maximum number of IP source address for filtering (per group) is 8.

  When there is no any source filtering address, the text *None* is shown in the **Source Address** field.
- **Type**: Indicates the Type. It can be either *Allow* or *Deny*.
- **Hardware Filter/Switch**: Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

Related Topics

Configuring MVR, on page 71

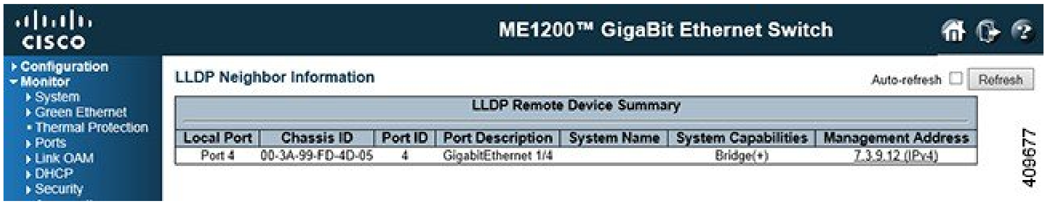
CHAPTER 43

Monitoring LLDP

The LLDP feature available on the ME 1200 Web GUI allows you to monitor the LLDP parameters, LLDP port, and LLDP Media.

LLDP Neighbor

This option provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected.



LLDP Neighbor Information

LLDP Remote Device Summary

Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
Port 4	00-3A-99-FD-4D-05	4	GigabitEthernet 1/4		Bridge(+)	7.3.9.12 (IPv4)

The columns hold the following information:

- **Local Port**: The port on which the LLDP frame was received.
- **Chassis ID**: The Chassis ID is the identification of the neighbor's LLDP frames.
- **Port ID**: The Port ID is the identification of the neighbor port.
- **Port Description**: Port Description is the port description advertised by the neighbor unit.
- **System Name**: System Name is the name advertised by the neighbor unit.
- **System Capabilities**: System Capabilities describes the neighbor unit's capabilities. The possible capabilities are:

1. *Other*
2. *Repeater*
3. *Bridge*
4. *WLAN Access Point*
5. *Router*
6. *Telephone*
7. *DOCSIS cable device*
8. *Station only*
9. *Reserved*
   When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

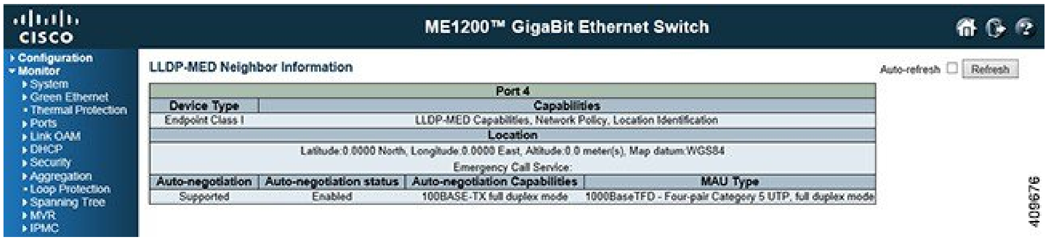
- **Management Address**: Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address.

Related Topics

Configuring LLDP, on page 75

LLDP-MED Neighbor Information

This option provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected.



LLDP-MED Neighbor Information

<table>
<tr><th colspan="4">Port 4</th></tr>
<tr><th>Device Type</th><th colspan="3">Capabilities</th></tr>
<tr><td>Endpoint Class I</td><td colspan="3">LLDP-MED Capabilities, Network Policy, Location Identification</td></tr>
<tr><th colspan="4">Location</th></tr>
<tr><td colspan="4">Latitude:0.0000 North, Longitude:0.0000 East, Altitude:0.0 meter(s), Map datum:WGS84
Emergency Call Service:</td></tr>
<tr><th>Auto-negotiation</th><th>Auto-negotiation status</th><th>Auto-negotiation Capabilities</th><th>MAU Type</th></tr>
<tr><td>Supported</td><td>Enabled</td><td>100BASE-TX full duplex mode</td><td>1000BaseTFD - Four-pair Category 5 UTP, full duplex mode</td></tr>
</table>

This function applies to VoIP devices which support LLDP-MED. The columns hold the following information:

- **Port**: The port on which the LLDP frame was received.
- **Device Type**: LLDP-MED Devices are comprised of two primary Device Types - Network Connectivity Devices and Endpoint Devices.

  LLDP-MED Network Connectivity Device Definition

  LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

  1. IEEE 802.1 Bridge
  2. IEEE 802.3 Repeater (included for historical reasons)
  3. IEEE 802.11 Wireless Access Point

4 LAN Switch/Router

5 Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method

LLDP-MED Endpoint Device Definition

LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework. Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.

Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

LLDP-MED Generic Endpoint (Class I)

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

LLDP-MED Media Endpoint (Class II)

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

LLDP-MED Communication Endpoint (Class III)

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.

- **LLDP-MED Capabilities**: LLDP-MED Capabilities describes the neighbor unit's LLDP-MED capabilities. The possible capabilities are:

1 LLDP-MED capabilities
2 Network Policy
3 Location Identification

4. Extended Power via MDI - PSE
5. Extended Power via MDI - PD
6. Inventory
7. Reserved

- **Application Type**: Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.

  1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
  2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media.
  3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
  4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.
  5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.
  6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
  7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
  8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media.

- **Policy**: Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either *Defined* or *Unknown*.

  - *Unknown*: The network policy for the specified application type is currently unknown.
  - *Defined*: The network policy is defined (known).

- **TAG**: TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be *Tagged* or *Untagged*.

  - *Untagged*: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.
  - *Tagged*: The device is using the IEEE 802.1Q tagged frame format.

- **VLAN ID**: VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

- **Priority**: Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).
- **DSCP**: DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).
- **Auto-negotiation**: Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.
- **Auto-negotiation status**: Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.
- **Auto-negotiation Capabilities**: Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.

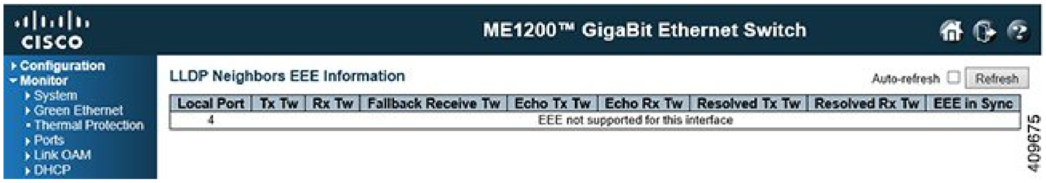
Related Topics

Configuring LLDP, on page 75

LLDP Neighbors EEE Information

By using EEE, power savings can be achieved at the expense of traffic latency. Due to that the circuits EEE turn off to save power, need time to boot up before sending traffic over the link. This time is called *wakeup time*. To achieve minimal latency, devices can use LLDP to exchange information about their respective tx and rx *wakeup time*, as a way to agree upon the minimum wakeup time they need.

This option provides an overview of EEE information exchanged by LLDP.



LLDP Neighbors EEE Information

Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
4	EEE not supported for this interface							

The displayed table contains a row for each port. If the port does not supports EEE, then it displays as **EEE not supported for this interface**.

If EEE is not enabled on particular interface, then it displays as **EEE not enabled for this interface**.

If the link partner does not supports EEE, then it displays as **Link partner is not EEE capable**.

The columns hold the following information:

- **Local Port**: The port on which LLDP frames are received or transmitted.
- **Tx Tw**: The link partner's maximum time that transmit path can hold-off sending data after deassertion of LPI.
- **Rx Tw**: The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.
- **Fallback Receive Tw**: The link partner's fallback receive Tw.

A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.

- **Echo Tx Tw**: The link partner's Echo Tx Tw value.

  The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.

- **Echo Rx Tw**: The link partner's Echo Rx Tw value.
- **Resolved Tx Tw**: The resolved Tx Tw for this link. Note : NOT the link partner.

  The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).

- **Resolved Rx Tw**: The resolved Rx Tw for this link. Note : NOT the link partner.

  The resolved value that is the actual **tx wakeup time** used for this link (based on EEE information exchanged via LLDP).

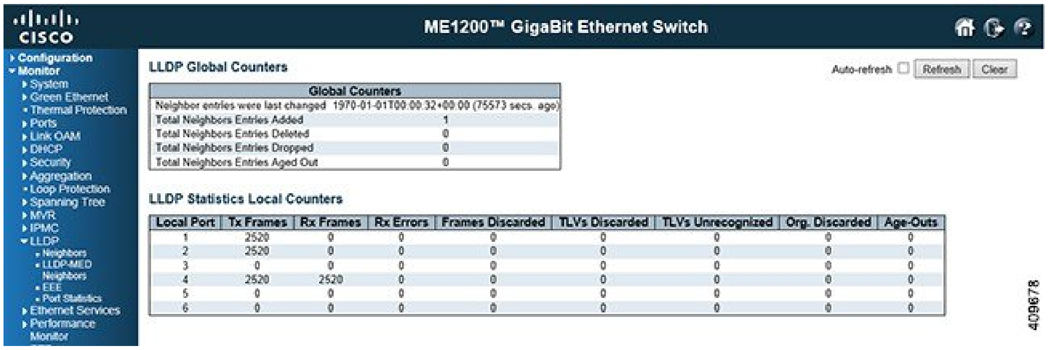
- **EEE in Sync**: Shows whether the switch and the link partner have agreed on wake times.
  - Red - Switch and link partner have not agreed on wakeup times.
  - Green - Switch and link partner have agreed on wakeup times.

Related Topics

Configuring LLDP, on page 75

LLDP Statistics

This option provides an overview of all LLDP traffic. Two types of counters are exist. Global counters are counters that refer to the whole switch, while local counters refer to per port counters for the currently selected switch.



LLDP Global Counters

Global Counters	
Neighbor entries were last changed	1970-01-01T00:00:32+00:00 (75573 secs. ago)
Total Neighbors Entries Added	1
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	2520	0	0	0	0	0	0	0
2	2520	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	2520	2520	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0

Global Counters

Displays Neighbor entries that were last changed: Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

- **Total Neighbors Entries Added**: Shows the number of new entries added since switch reboot.
- **Total Neighbors Entries Deleted**: Shows the number of new entries deleted since switch reboot.
- **Total Neighbors Entries Dropped**: Shows the number of LLDP frames dropped due to the entry table being full.
- **Total Neighbors Entries Aged Out**: Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The table contains a row for each port. The columns hold the following information:

- **Local Port**: The port on which LLDP frames are received or transmitted.
- **Tx Frames**: The number of LLDP frames transmitted on the port.
- **Rx Frames**: The number of LLDP frames received on the port.
- **Rx Errors**: The number of received LLDP frames containing some kind of error.
- **Frames Discarded**: If a LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as *Too Many Neighbors* in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are remove from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.
- **TLVs Discarded**: Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
- **TLVs Unrecognized**: The number of well-formed TLVs, but with an unknown type value.
- **Org. Discarded**: If LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted.
- **Age-Outs**: Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

Related Topics

Configuring LLDP, on page 75

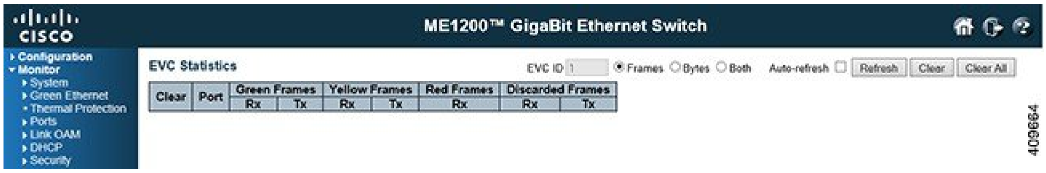
CHAPTER 44

Monitoring Ethernet Services

The Ethernet Services feature available on the ME 1200 Web GUI allows you to monitor the EVC port, EVC L2CP, EVC bandwidth, and EVC Control List.

EVC Statistics

This option provides NNI port traffic statistics for the selected EVC. It also shows counters for UNI ports of ECEs mapping to the EVC.



EVC Statistics

EVC ID 1 ● Frames ○ Bytes ○ Both Auto-refresh □

Clear	Port	Green Frames		Yellow Frames		Red Frames	Discarded Frames	
		Rx	Tx	Rx	Tx	Rx	Rx	Tx

- **Clear**: This box is used to mark a port for clearance in next Clear operation.
- **Port**: The UNI/NNI port for the EVC.
- **Rx Green**: The number of green received.
- **Tx Green**: The number of green transmitted.
- **Rx Yellow**: The number of yellow received.
- **Tx Yellow**: The number of yellow transmitted.
- **Rx Red**: The number of red received.
- **Rx Discarded**: The number of discarded in the ingress queue system.
- **Tx Discarded**: The number of discarded in the egress queue system.
- **Frames**: Show frames statistics only.

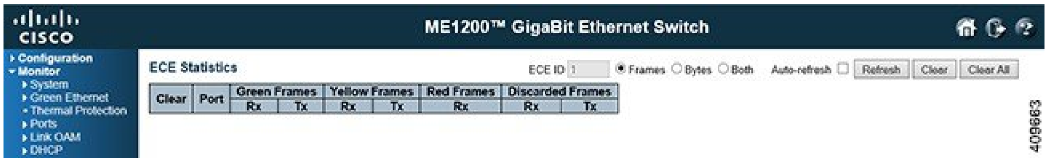
- **Bytes**: Show bytes statistics only.
- **Both**: Show both frames and bytes statistics.

Related Topics

Configuring Ethernet Services, on page 103

ECE Statistics

This option provides UNI port traffic statistics for available ECE. It also shows counters for NNI ports of the EVC to which the ECE is mapped.



ECE Statistics

ECE ID 1 ● Frames ○ Bytes ○ Both Auto-refresh □

Clear	Port	Green Frames		Yellow Frames		Red Frames	Discarded Frames	
		Rx	Tx	Rx	Tx	Rx	Rx	Tx

- **Clear**: This box is used to mark a port for clearance in next Clear operation.
- **Port**: The UNI/NNI port for the ECE.
- **Rx Green Frames and Bytes**: The number of green bytes and frames received.
- **Tx Green Frames and Bytes**: The number of green bytes and frames transmitted.
- **Rx Yellow Frames and Bytes**: The number of yellow bytes and frames received.
- **Tx Yellow Frames and Bytes**: The number of yellow bytes and frames transmitted.
- **Rx Red Frames and Bytes**: The number of red bytes and frames received.
- **Rx Discarded Frames and Bytes**: The number of bytes and frames discarded in the ingress queue system.
- **Tx Discarded Frames and Bytes**: The number of bytes and frames discarded in the egress queue system.
- **Frames**: Show frames statistics only.
- **Bytes**: Show bytes statistics only.
- **Both**: Show both frames and bytes statistics.

Related Topics

Configuring Ethernet Services, on page 103

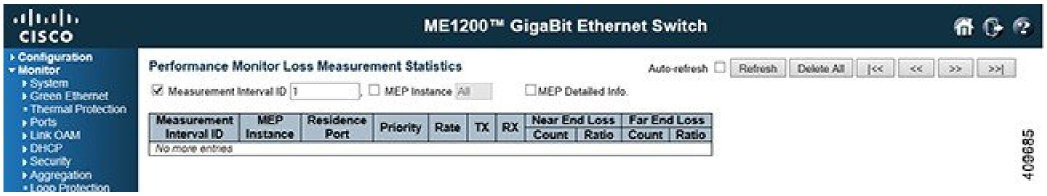
CHAPTER 45

Monitoring Performance Monitor

The Performance Monitor feature available on the ME 1200 Web GUI allows you to monitor the Performance Monitor statistics.

Performance Monitor Loss Measurement Statistics

This option provides the performance monitor loss measurement traffic statistics for the selected measurement interval ID and Loss Measurement instance.



Performance Monitor Loss Measurement Statistics

☑ Measurement Interval ID 1 , □ MEP Instance All □MEP Detailed Info.

Measurement Interval ID	MEP Instance	Residence Port	Priority	Rate	TX	RX	Near End Loss		Far End Loss	
							Count	Ratio	Count	Ratio
No more entries										

- **Measurement Interval ID**: The measurement interval for the performance monitor data sets.
- **MEP Instance**: The MEP instance for the performance monitor data sets.
- **Residence Port**: The residence port for the MEP.
- **Priority**: The priority to be inserted as PCP bits in TAG (if any).
- **Rate**: The gap between transmitting 1DM/DMM PDU in 10 ms. The range is 10 to 65535.
- **Unit**: The time resolution.
- **TX**: The number of frame transmitted.
- **RX**: The number of frame received.

- **One-way Far to Near Average Delay**: The one-way far to near average delay.
- **One-way Far to Near Average Delay Variation**: The one-way far to near average delay variation.
- **One-way Far to Near Min. Delay**: The minimum one-way near to far delay.
- **One-way Far to Near Max. Delay**: The maximum one-way near to far delay.
- **One-way Near to Far Average Delay**: The number of red received.
- **One-way Near to Far Average Delay Variation**: The one-way near to far average delay variation.
- **One-way Near to Far Min. Delay**: The minimum one-way near to far delay.
- **One-way Near to Far Max. Delay**: The maximum one-way near to far delay.
- **Two-way Delay Average Delay**: The two-way average delay.
- **Two-way Average Delay Variation**: The two-way average delay variation.
- **Two-way Min. Delay**: The minimum two-way delay.
- **Two-way Max. Delay**: The maximum two-way delay.
- **Domain**
    - **Port**: This is a MEP in the Port Domain. **Flow Instance** is a Port.
    - **Evc**: This is a MEP in the EVC Domain. **Flow Instance** is an EVC.
    - **VLAN**: This is a MEP in the VLAN Domain. **Flow Instance** is a VLAN.
- **Direction**
    - *Up*: This is a Down MEP - monitoring ingress OAM and traffic on **Residence Port**.
    - *Down*: This is a Up MEP - monitoring egress OAM and traffic on **Residence Port**.
- **Level**: The MEG level of this MEP.
- **Flow Instance**: The MEP is related to this flow - See **Domain**.
- **Tagged VID**
    - **Port MEP**: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.
    - **EVC MIP**: On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active.
- **MEP ID**: This value will become the transmitted two byte CCM MEP ID.
- **MAC Address**: The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).
- **Peer MEP ID**: This value will become an expected MEP ID in a received CCM - see **cMEP**.
- **Peer MAC Address**: This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP.
- **Bin**: A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

If the measurement threshold is 5000 microseconds and the total number of Measurement Bins is four, we can give an example as follows:

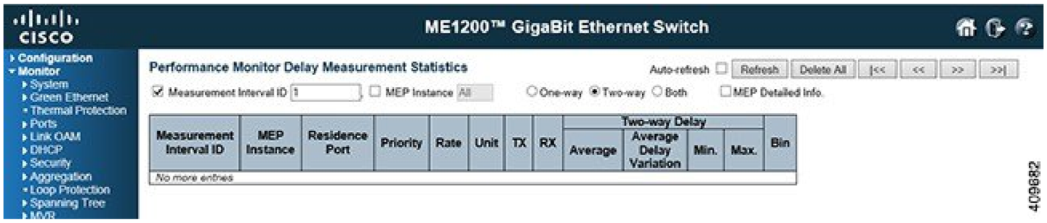
Bin	Threshold	Range
bin0	0 microsecond	0 microsecond <= measurement < 5,000 microseconds
bin1	5,000 microseconds	5,000 microseconds <= measurement < microseconds
bin2	10,000 microseconds	10,000 microseconds <= measurement < 15,000 microseconds
bin3	15,000 microseconds	15,000 microseconds <= measurement < infinite microseconds

Related Topics

Configuring Performance Monitor, on page 111

Performance Monitor Delay Measurement Statistics

This option provides the performance monitor delay measurement traffic statistics for the selected measurement interval ID and Delay Measurement instance.



Performance Monitor Delay Measurement Statistics

☑ Measurement Interval ID 1 □ MEP Instance All ○ One-way ● Two-way ○ Both □ MEP Detailed Info.

Measurement Interval ID	MEP Instance	Residence Port	Priority	Rate	Unit	TX	RX	Two-way Delay				Bin
								Average	Average Delay Variation	Min.	Max.	
No more entries												

- **Measurement Interval ID**: The measurement interval for the performance monitor data sets.
- **MEP Instance**: The MEP instance for the performance monitor data sets.
- **Residence Port**: The residence port for the MEP.
- **Priority**: The priority to be inserted as PCP bits in TAG (if any).
- **Rate**: Selected the frame rate of CCM/LMM PDU. This is the inverse of transmission period as described in Y.1731.
- **TX**: The number of frame transmitted. RXThe number of frame received.
- **Near End Loss Count**: The near end loss count.
- **Near End Loss Ratio**: The near end loss ratio.
- **Far End Loss Count**: The far end loss count.

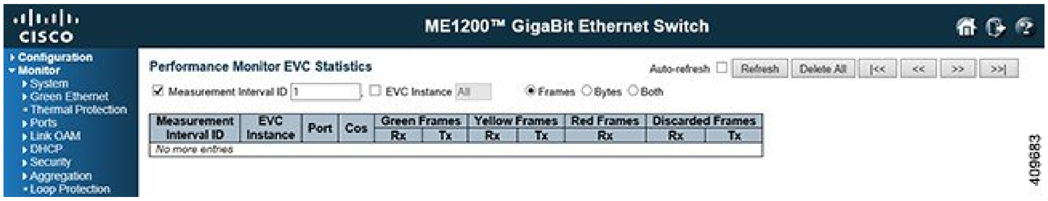
- **Far End Loss Ratio**: The far end loss ratio.
- **Domain**
    - **Port**: This is a MEP in the Port Domain. **Flow Instance** is a Port.
    - **Evc**: This is a MEP in the EVC Domain. **Flow Instance** is an EVC.
    - **VLAN**: This is a MEP in the VLAN Domain. **Flow Instance** is a VLAN.
- **Direction**
    - *Up*: This is a Down MEP - monitoring ingress OAM and traffic on **Residence Port**.
    - *Down*: This is a Up MEP - monitoring egress OAM and traffic on **Residence Port**.
- **Level**: The MEG level of this MEP.
- **Flow Instance**: The MEP is related to this flow - See **Domain**.
- **Tagged VID**
    - **Port MEP**: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.
    - **EVC MIP**: On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active.
- **MEP ID**: This value will become the transmitted two byte CCM MEP ID.
- **MAC Address**: The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

Related Topics

Configuring Performance Monitor, on page 111

Performance Monitor EVC Statistics

This option provides the performance monitor EVC traffic statistics for the selected measurement interval ID and EVC instance.



Performance Monitor EVC Statistics

☑ Measurement Interval ID 1 □ EVC Instance All ● Frames ○ Bytes ○ Both

Measurement Interval ID	EVC Instance	Port	Cos	Green Frames		Yellow Frames		Red Frames	Discarded Frames	
				Rx	Tx	Rx	Tx	Rx	Rx	Tx
No more entries										

- **Measurement Interval ID**: The measurement interval for the performance monitor data sets.
- **EVC Instance**: The EVC instance for the performance monitor data sets.
- **MEP Instance**: The MEP instance for the performance monitor data sets.
- **Residence Port**: The residence port for the EVC.

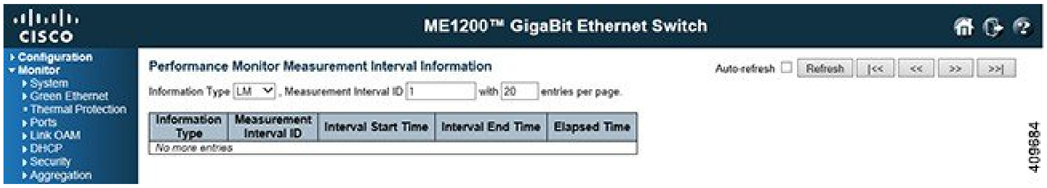
- **Cos**
    - **NNI na**: this is the NNI port and counters are not per Cos on this port.
    - **UNI 0-7**: this is the UNI port and counters are per Cos on this port.
- **Rx Green Frames**: The number of green received.
- **Tx Green Frames**: The number of green transmitted.
- **Rx Yellow Frames**: The number of yellow received.
- **Tx Yellow Frames**: The number of yellow transmitted.
- **Rx Red Frames**: The number of red received.
- **Rx Discarded Frames**: The number of discarded in the ingress queue system.
- **Tx Discarded Frames**: The number of discarded in the egress queue system.
- **Frames**: Show frames statistics only.
- **Bytes**: Show bytes statistics only.
- **Both**: Show both frames and bytes statistics.

Related Topics

Configuring Performance Monitor, on page 111

Performance Monitor Measurement Interval Information

This option provides the performance monitor measurement interval information.



Performance Monitor Measurement Interval Information

Information Type LM, Measurement Interval ID 1 with 20 entries per page.

Information Type	Measurement Interval ID	Interval Start Time	Interval End Time	Elapsed Time
No more entries				

- **Information Type**: The type for the performance monitor data sets.
- **Measurement Interval ID**: The measurement interval for the performance monitor data sets.
- **Interval Start Time**: The interval start time.
- **Interval End Time**: The interval end time.
- **Elapsed Time**: The elapsed time.

Related Topics

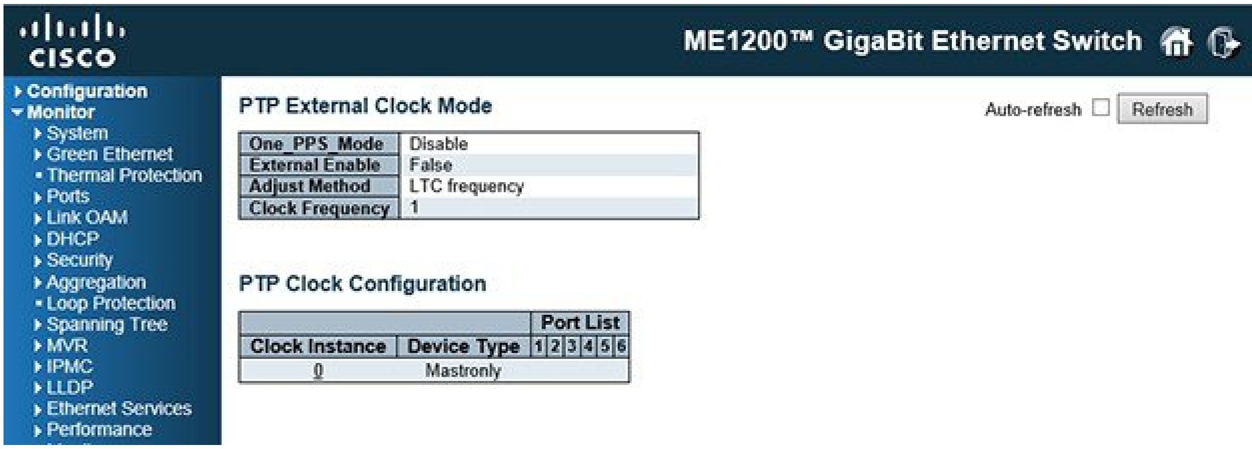
Configuring Performance Monitor, on page 111

CHAPTER 46

Monitoring PTP

PTP Clock Monitor

This option allows you to inspect the current PTP clock settings.



PTP External Clock Mode

One_PPS_Mode	Disable
External Enable	False
Adjust Method	LTC frequency
Clock Frequency	1

PTP Clock Configuration

		Port List					
Clock Instance	Device Type	1	2	3	4	5	6
0	Mastronly						

PTP External Clock Description

- **One_PPS_Mode**: Shows the current One_pps_mode configured.

  1. *Output*: Enable the 1 pps clock output
  2. *Input*: Enable the 1 pps clock input
  3. *Disable* : Disable the 1 pps clock in/out-putExternal

- Enable: Shows the current External clock output configuration.

  - *True* : Enable the external clock output
  - *False* : Disable the external clock outputAdjust

- Method: Shows the current Frequency adjustment configuration.

1. **LTC frequency** : Local Time Counter (LTC) frequency control.
2. **SyncE-DPLL** : SyncE DPLL frequency control, if allowed by SyncE.
3. **Oscillator** : Oscillator independent of SyncE for frequency control, if supported by the HW.
4. **LTC phase** : Local Time Counter (LTC) phase control (assumes that the frequency is locked by means of SyncE).

- **Clock Frequency**: Shows the current clock frequency used by the External Clock.The possible range of values are 1 - 25000000 (1 - 25MHz).

PTP Clock Description

- **Inst**: Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to monitor the Clock details.
- **ClkDom**: Indicates the Clock domain used by the Instance of a particular Clock Instance [0..3].
- **Device Type**: Indicates the Type of the Clock Instance. There are five Device Types.

1. Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock.
2. P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock.
3. E2e Transp - Clock's Device Type is End to End Transparent Clock.
4. Master Only - Clock's Device Type is Master Only.
5. Slave Only - Clock's Device Type is Slave Only.

- **Port List**: Shows the ports configured for that Clock Instance.

Related Topics

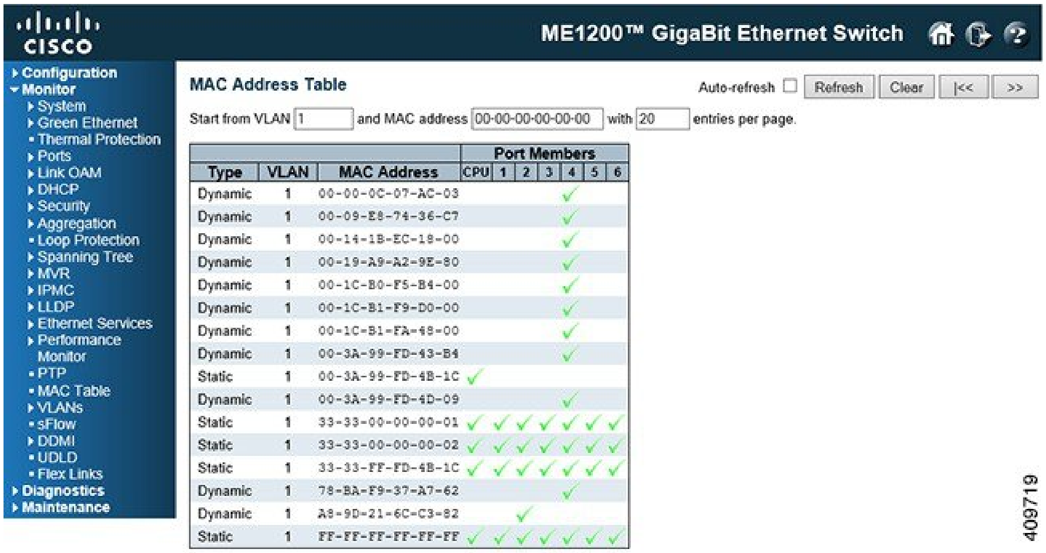
Configuring PTP, on page 133

CHAPTER 47

Monitoring MAC Table

Dynamic MAC Table

This option displays entries in the MAC Table. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.



MAC Address Table

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

			Port Members						
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6
Dynamic	1	00-00-0C-07-AC-03					✓		
Dynamic	1	00-09-E8-74-36-C7					✓		
Dynamic	1	00-14-1B-EC-18-00					✓		
Dynamic	1	00-19-A9-A2-9E-80					✓		
Dynamic	1	00-1C-B0-F5-B4-00					✓		
Dynamic	1	00-1C-B1-F9-D0-00					✓		
Dynamic	1	00-1C-B1-FA-48-00					✓		
Dynamic	1	00-3A-99-FD-43-B4					✓		
Static	1	00-3A-99-FD-4B-1C	✓						
Dynamic	1	00-3A-99-FD-4D-09					✓		
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-FD-4B-1C	✓	✓	✓	✓	✓	✓	✓
Dynamic	1	78-BA-F9-37-A7-62					✓		
Dynamic	1	A8-9D-21-6C-C3-82			✓				
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓

Navigating the MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the **entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The **Start from MAC address** and **VLAN** input fields allow the user to select the starting point in the MAC Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next MAC

Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text **No more entries** is shown in the displayed table. Use the **|<<** button to start over.

MAC Table Columns

- **Type**: Indicates whether the entry is a static or a dynamic entry.
- **MAC address**: The MAC address of the entry.
- **VLAN**: The VLAN ID of the entry.
- **Port Members**: The ports that are members of the entry.

Related Topics

Configuring MAC Table, on page 95

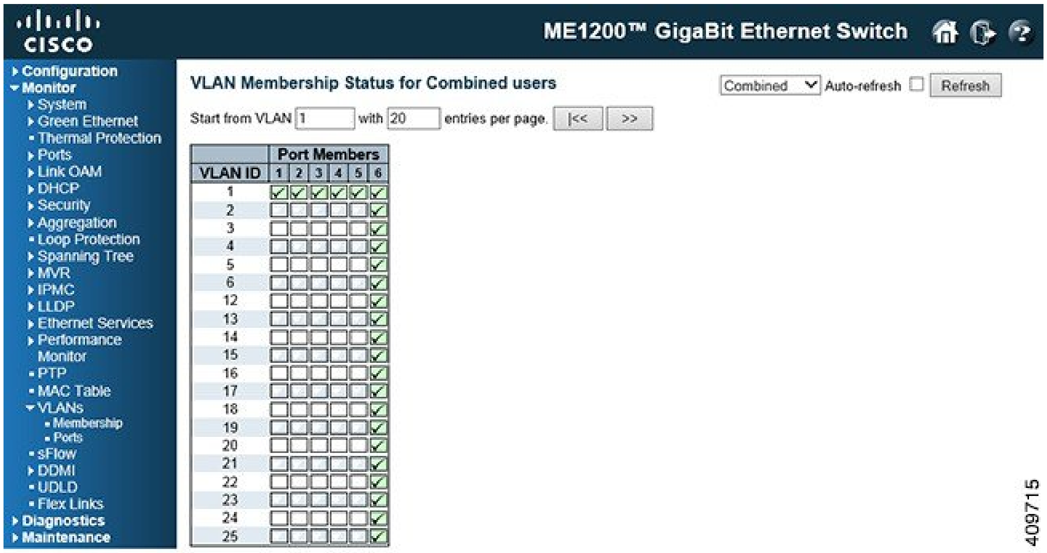
CHAPTER 48

Monitoring VLANs

The VLANs feature available on the ME 1200 Web GUI allows you to monitor the VLAN membership and port status for VLAN users.

VLAN Membership Status

This option provides an overview of membership status of VLAN users.



VLAN Membership Status for Combined users

Combined ▾ Auto-refresh □

Start from VLAN 1 with 20 entries per page.

	Port Members					
VLAN ID	1	2	3	4	5	6
1	☑	☑	☑	☑	☑	☑
2	□	□	□	□	□	☑
3	□	□	□	□	□	☑
4	□	□	□	□	□	☑
5	□	□	□	□	□	☑
6	□	□	□	□	□	☑
12	□	□	□	□	□	☑
13	□	□	□	□	□	☑
14	□	□	□	□	□	☑
15	□	□	□	□	□	☑
16	□	□	□	□	□	☑
17	□	□	□	□	□	☑
18	□	□	□	□	□	☑
19	□	□	□	□	□	☑
20	□	□	□	□	□	☑
21	□	□	□	□	□	☑
22	□	□	□	□	□	☑
23	□	□	□	□	□	☑
24	□	□	□	□	□	☑
25	□	□	□	□	□	☑

- **VLAN User**: Various internal software modules may use VLAN services to configure VLAN memberships on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.

The **Combined** entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

- **VLAN ID**: VLAN ID for which the Port members are displayed.
- **Port Members**: A row of check boxes for each port is displayed for each VLAN ID.
  - If a port is included in a VLAN, a check will be displayed.
  - If a port is in the forbidden port list, a cross will be displayed.
  - If a port is in the forbidden port list and at the same time attempted included in the VLAN, the following image will be displayed: conflict port. The port will not be a member of the VLAN in this case.

Navigating the VLAN Membership Status page

Each page shows up to 99 entries from the VLAN table (default being 20), selected through the **entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The **VLAN** input field allows the user to select the starting point in the VLAN Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next VLAN Table match.

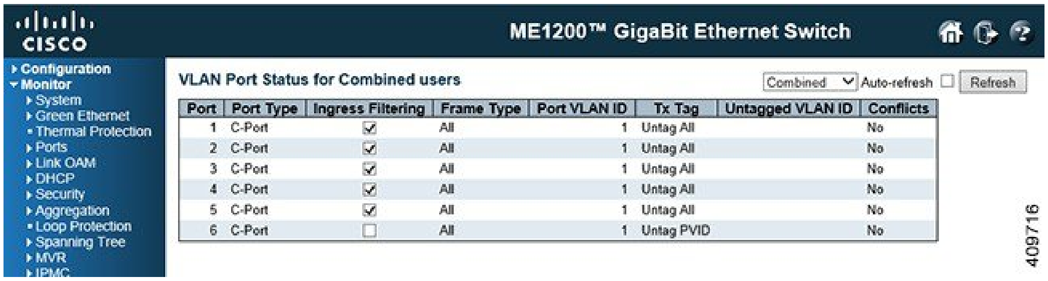
The >> will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached, the text **No data exists for the selected user** is shown in the table. Use the **|<<** button to start over.

Related Topics

Configuring VLANs, on page 97

VLAN Port Status

This option provides VLAN Port Status.



VLAN Port Status for Combined users

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	1	Untag All		No
2	C-Port	☑	All	1	Untag All		No
3	C-Port	☑	All	1	Untag All		No
4	C-Port	☑	All	1	Untag All		No
5	C-Port	☑	All	1	Untag All		No
6	C-Port	□	All	1	Untag PVID		No

- **VLAN User**: Various internal software modules may use VLAN services to configure VLAN port configuration on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.

  The **Combined** entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware. If a given software modules has not overridden any of the port settings, the text **No data exists for the selected user** is shown in the table.

- **Port**: The logical port for the settings contained in the same row.
- **Port Type**: Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port.) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.
- **Ingress Filtering**: Shows whether a given user wants ingress filtering enabled or not. The field is empty if not overridden by the selected user.
- **Frame Type**: Shows the acceptable frame types (All, Taged, Untagged) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.
- **Port VLAN ID**: Shows the Port VLAN ID (PVID) that a given user wants the port to have. The field is empty if not overridden by the selected user.
- **Tx Tag**: Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port.The field is empty if not overridden by the selected user.
- **Untagged VLAN ID**: If Tx Tag is overridden by the selected user and is set to Tag or Untag UVID, then this field will show the VLAN ID the user wants to tag or untag on egress. The field is empty if not overridden by the selected user.
- **Conflicts**: Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress.

  Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list: The higher in the list, the higher priority. If conflicts exist, it will be displayed as *Yes* for the *Combined* user and the offending software module. The **Combined** user reflects what is actually configured in hardware.

Related Topics

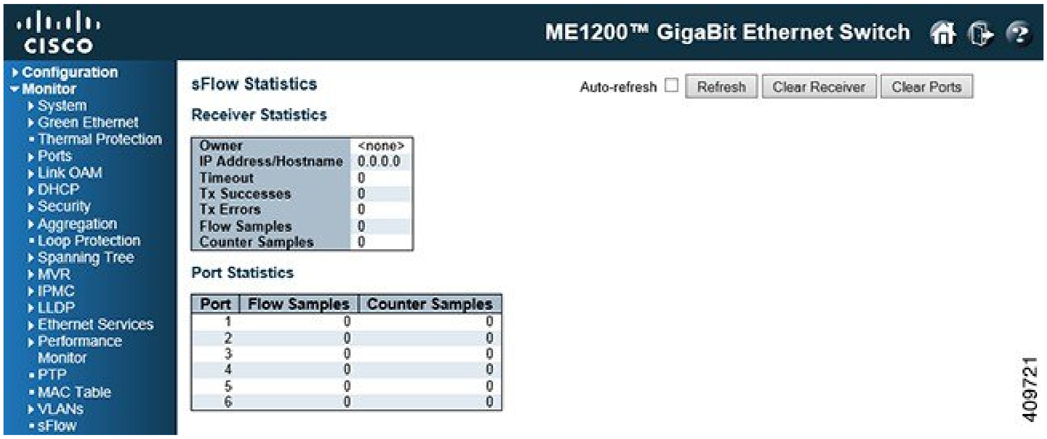
Configuring VLANs, on page 97

CHAPTER 49

Monitoring sFlow

sFlow Statistics

This option shows receiver and per-port sFlow statistics.



sFlow Statistics

Receiver Statistics

Owner	<none>
IP Address/Hostname	0.0.0.0
Timeout	0
Tx Successes	0
Tx Errors	0
Flow Samples	0
Counter Samples	0

Port Statistics

Port	Flow Samples	Counter Samples
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0

Receiver Statistics

- **Owner**: This field shows the current owner of the sFlow configuration. It assumes one of three values as follows:
  - If sFlow is currently unconfigured/unclaimed, Owner contains *none*.
  - If sFlow is currently configured through Web or CLI, Owner contains **Configured through local management**.
  - If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.
- **IP Address/Hostname**: The IP address or hostname of the sFlow receiver.

- **Timeout**: The number of seconds remaining before sampling stops and the current sFlow owner is released.
- **Tx Successes**: The number of UDP datagrams successfully sent to the sFlow receiver.
- **Tx Errors**: The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics ? Ping/Ping6).
- **Flow Samples**: The total number of flow samples sent to the sFlow receiver. Counter SamplesThe total number of counter samples sent to the sFlow receiver.

Port Statistics

- **Port**: The port number for which the following statistics applies.
- **Flow Samples**: The number of flow samples sent to the sFlow receiver originating from this port.
- **Counter Samples**: The total number of counter samples sent to the sFlow receiver originating from this port.

Related Topics

sFlow Configuration, on page 141

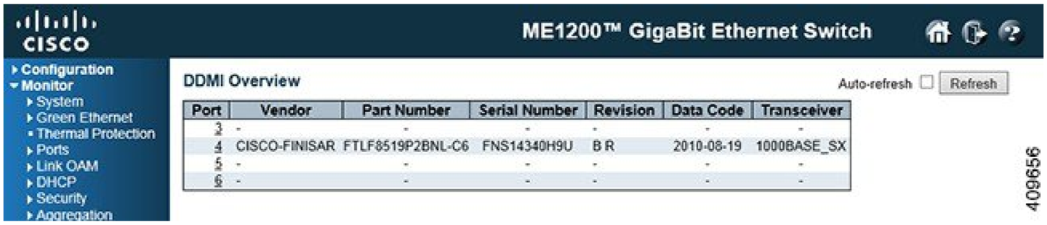
CHAPTER 50

Monitoring DDMI

The DDMI feature available on the ME 1200 Web GUI allows you to monitor the DDMI information for the ME 1200 switch.

DDMI Overview

This options provides an overview of DDMI feature.



DDMI Overview

Auto-refresh □ Refresh

Port	Vendor	Part Number	Serial Number	Revision	Data Code	Transceiver
3	-	-	-	-	-	-
4	CISCO-FINISAR	FTLF8519P2BNL-C6	FNS14340H9U	B R	2010-08-19	1000BASE_SX
5	-	-	-	-	-	-
6	-	-	-	-	-	-

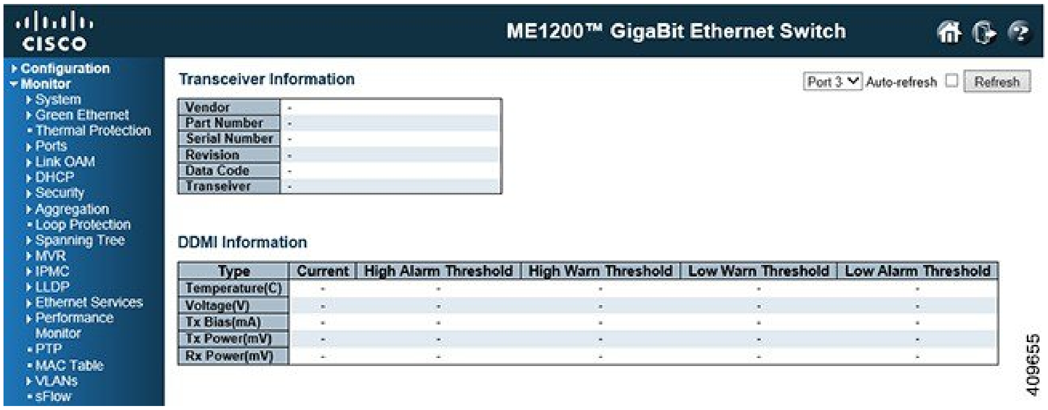
- **Port**: DDMI port.
- **Vendor**: Indicates Vendor name SFP vendor name.
- **Part Number**: Indicates Vendor PN Part number provided by SFP vendor.
- **Serial Number**: Indicates Vendor SN Serial number provided by vendor.
- **Revision**: Indicates Vendor rev Revision level for part number provided by vendor.
- **Data Code**: Indicates Date code Vendor¡¦s manufacturing date code.
- **Transeiver**: Indicates Transceiver compatibility.

Related Topics

Configuring DDMI, on page 163

DDMI Detailed

This option explains information on the DDMI feature in detail.



Transceiver Information

Vendor	-
Part Number	-
Serial Number	-
Revision	-
Data Code	-
Transeiver	-

DDMI Information

Type	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)	-	-	-	-	-
Voltage(V)	-	-	-	-	-
Tx Bias(mA)	-	-	-	-	-
Tx Power(mV)	-	-	-	-	-
Rx Power(mV)	-	-	-	-	-

Transceiver Information

- **Vendor**: Indicates Vendor name SFP vendor name.
- **Part Number**: Indicates Vendor PN Part number provided by SFP vendor.
- **Serial Number**: Indicates Vendor SN Serial number provided by vendor.
- **Revision**: Indicates Vendor rev Revision level for part number provided by vendor.
- **Data Code**: Indicates Date code Vendor¡¦s manufacturing date code.
- **Transeiver**: Indicates Transceiver compatibility.

DDMI Infomration

- **Current**: The current value of temperature, voltage, TX bias, TX power, and RX power.
- **High Alarm Threshold**: The high alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.
- **High Warn Threshold**: The high warn threshold value of temperature, voltage, TX bias, TX power, and RX power.
- **Low Warn Threshold**: The low warn threshold value of temperature, voltage, TX bias, TX power, and RX power.
- **Low Alarm Threshold**: The low alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.

Related Topics

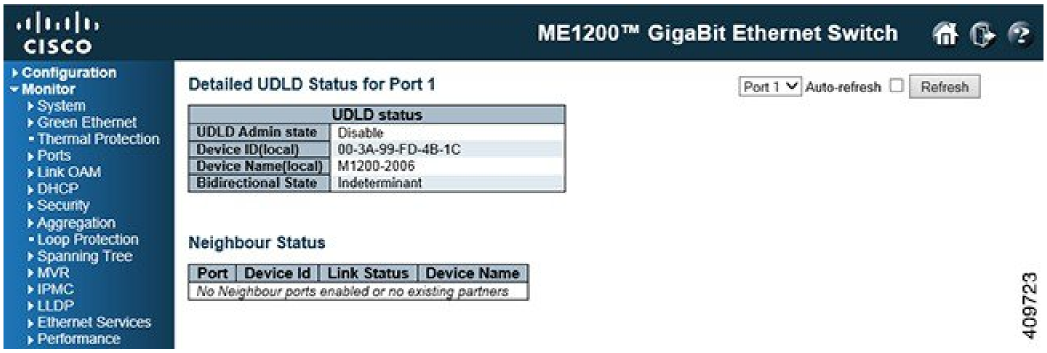
Configuring DDMI, on page 163

CHAPTER 51

Monitoring UDLD

UDLD Status

This option displays the UDLD status of the ports.



Detailed UDLD Status for Port 1

UDLD status	
UDLD Admin state	Disable
Device ID(local)	00-3A-99-FD-4B-1C
Device Name(local)	M1200-2006
Bidirectional State	Indeterminant

Neighbour Status

Port	Device Id	Link Status	Device Name
No Neighbour ports enabled or no existing partners			

UDLD port status

- **UDLD Admin State**: The current port state of the logical port, *Enabled* if any of the state(*Normal, Aggressive*) is enabled.
- **Device ID**(local): The ID of Device.
- **Device Name**(local): Name of the Device.
- **Bidirectional State**: The current state of the port.

Neighbour Status

- **Port**: The current port of neighbour device.
- **Device ID**: The current ID of neighbour device.
- **Link Status**: The current link status of neighbour port.

- **Device Name**: Name of the Neighbour Device.

Related Topics

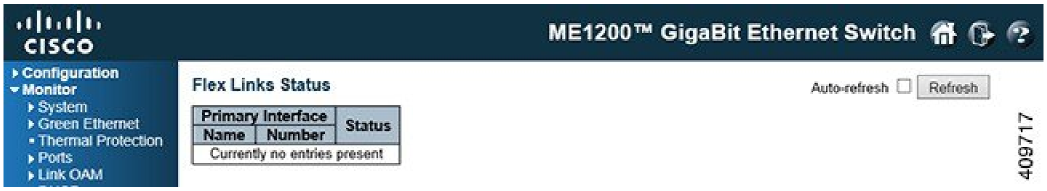
Configuring UDLD, on page 165

CHAPTER 52

Monitoring Flex Links

Flex Links Status

This option provides information on each of the Flex Links pair status. Each flex link entry is represented by its primary interface.



Flex Links Status

Primary Interface		Status
Name	Number	
Currently no entries present		

- **Primary Interface**: This represents flex links pair by the primary interface in **Name** and **Number**. Name tells whether it is a port interface or port channel interface, and number shows the port number or group id of the interface. The flex links pair represented can be configured in configuration page.
- **Status**: Status shows the current flex links primary and backup interface link status. The default status is **Active Up/Backup Standby**, If a link failure has occurred on primary interface, the interface forwarding state will be given to backup interface, and therefore the status will be **Active Standby/Backup Up**.

Related Topics

Configuring Flex Links, on page 167

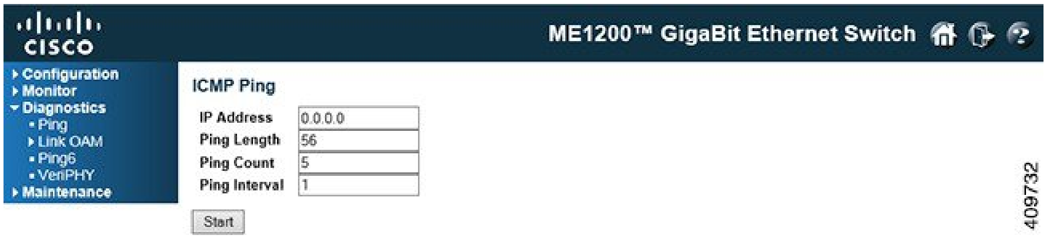
CHAPTER 53

Diagnostics

The Diagnostics feature available on the ME 1200 Web GUI allows you to perform diagnostic procedures on the ME 1200 switch.

Ping

This option allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.



ICMP Ping

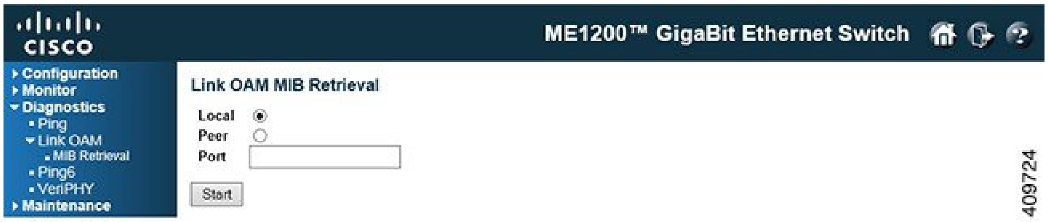
IP Address 0.0.0.0
Ping Length 56
Ping Count 5
Ping Interval 1

After you the press **Start** button, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested data space(the ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
PING server 10.10.132.20, 56 bytes of data.
64 bytes from 10.10.132.20: icmp_seq=0, time=0ms
64 bytes from 10.10.132.20: icmp_seq=1, time=0ms
64 bytes from 10.10.132.20: icmp_seq=2, time=0ms
64 bytes from 10.10.132.20: icmp_seq=3, time=0ms
64 bytes from 10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

Link OAM MIB Retrieval

This option allows you to retrieve the local or remote OAM MIB variable data on a particular port. Select the appropriate radio button and enter the port number of the switch to retrieve the content of interest. Click on the **Start** button to retrieve the content. Click on the **New Retrieval** button to retrieve another content of interest.

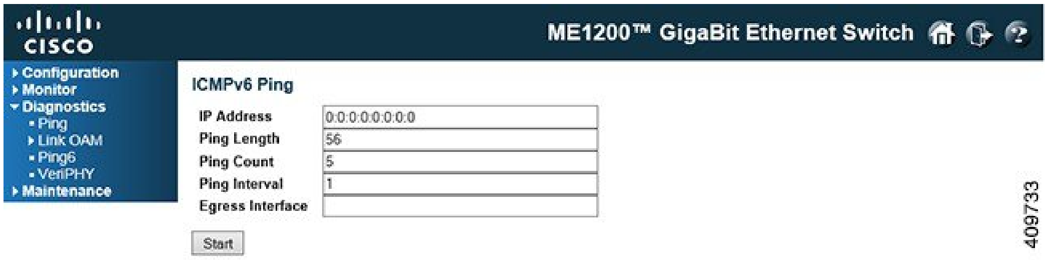


Link OAM MIB Retrieval

Local ●
Peer ○
Port

Ping6

This option allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues. After you press Start, ICMPv6 packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.



ICMPv6 Ping

IP Address: 0:0:0:0:0:0:0:0
Ping Length: 56
Ping Count: 5
Ping Interval: 1
Egress Interface:

```
PING6 server ff02::2, 56 bytes of data.
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=0, time=10ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=0, time=10ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=1, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=1, time=0ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=2, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=2, time=0ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=3, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=3, time=0ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=4, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=4, time=0ms
Sent 5 packets, received 10 OK, 0 bad
```

You can configure the following properties of the issued ICMP packets.

- **IP Address**: The destination IP Address.
- **Ping Length**: The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
- **Ping Count**: The count of the ICMP packet. Values range from 1 time to 60 times.

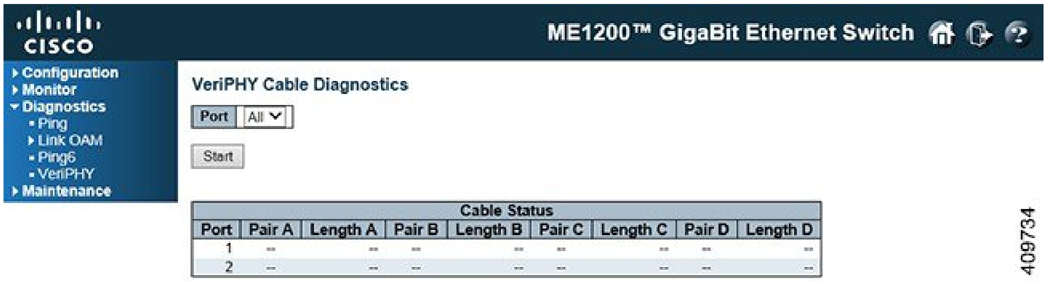
- **Ping Interval**: The interval of the ICMP packet. Values range from 0 second to 30 seconds
- **Egress Interface** (Only for IPv6): The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes.The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. When the egress interface is not given, PING6 finds the best match interface for destination.

  Do not specify egress interface for loopback address.

  Do specify egress interface for link-local or multicast address.

VeriPHY

This option is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.



Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--

Press the **Start** button to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters.

10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

- **Port**: The port where you are requesting VeriPHY Cable Diagnostics.
- **Port**: Port number.
- **Pair**: The status of the cable pair.

OK	Correctly terminated pair
Open	Open pair
Short	Shorted pair
Short A	Cross-pair short to pair A
Short B	Cross-pair short to pair B
Short C	Cross-pair short to pair C
Short D	Cross-pair short to pair D
Cross A	Abnormal cross-pair coupling with pair A
Cross B	Abnormal cross-pair coupling with pair B

Cross C	Abnormal cross-pair coupling with pair C
Cross D	Abnormal cross-pair coupling with pair D

- **Length**: The length (in meters) of the cable pair. The resolution is 3 meters.

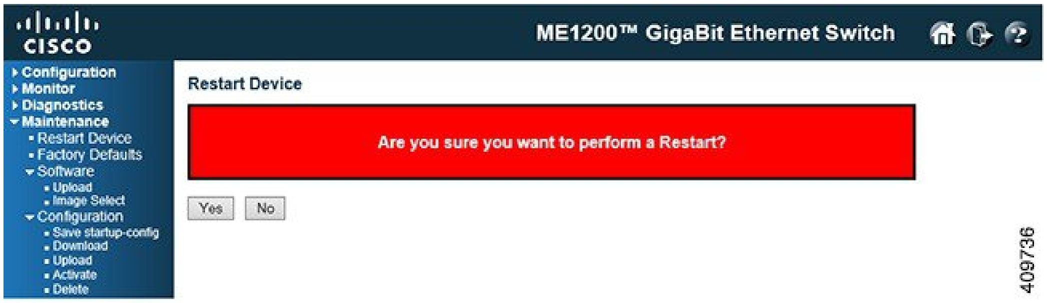
CHAPTER 54

Maintenance

The Maintenance feature available on the ME 1200 Web GUI allows you to perform maintenance procedures on the ME 1200 switch.

Restart Device

You can restart the switch with this option. After restart, the switch will boot normally.



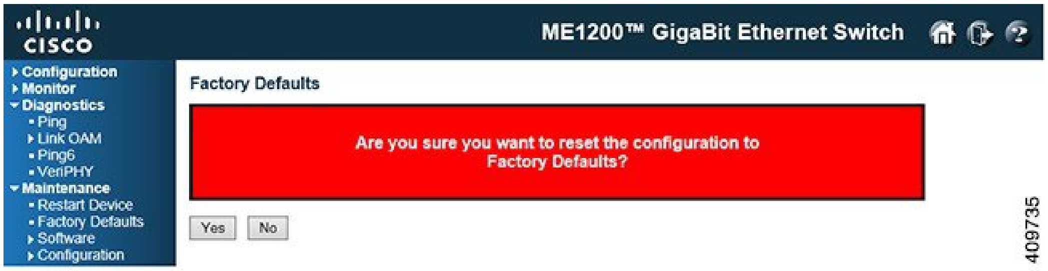
Restart Device

Are you sure you want to perform a Restart?

- Click **Yes**to restart device.
- Click **No** to return to the Port State page without restarting.

Factory Defaults

You can reset the configuration of the switch with this option. Only the IP configuration is retained.



Factory Defaults

Are you sure you want to reset the configuration to Factory Defaults?

Yes No

The new configuration is available immediately, which means that no restart is necessary.

- Click **Yes** to reset the configuration to Factory Defaults.
- Click **No** to return to the Port State page without resetting the configuration.

Note Restoring factory default can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, 'loopback' packets will be transmitted at port 1. If a 'loopback' packet is received at port 2 the switch will do a restore to default.

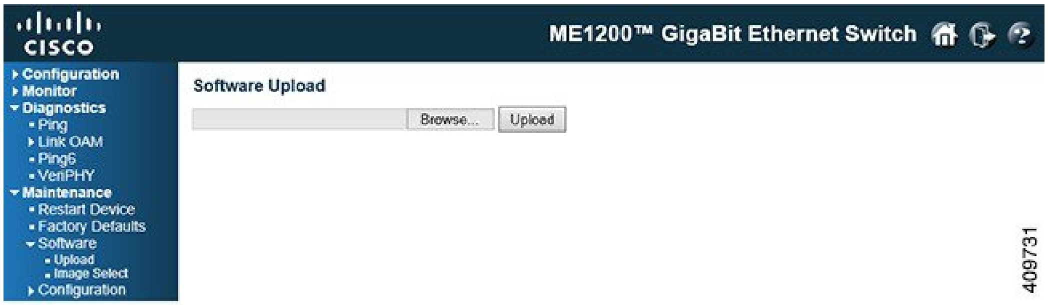
Related Topics

Reset Configuration to Factory Defaults, on page 2

Software

Software Upload

This option facilitates an update of the firmware controlling the switch.



Software Upload

Browse to the location of a software image and click **Upload**.

After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.

Warning: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.

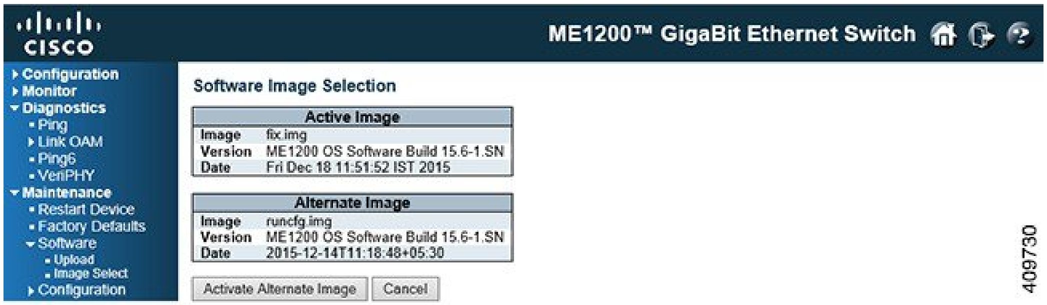
Related Topics

Software Upgrade, on page 2

Firmware Selection

This option provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

Displays two tables with information about the active and alternate firmware images.



Software Image Selection

Active Image	
Image	fix.img
Version	ME1200 OS Software Build 15.6-1.SN
Date	Fri Dec 18 11:51:52 IST 2015

Alternate Image	
Image	runcfg.img
Version	ME1200 OS Software Build 15.6-1.SN
Date	2015-12-14T11:18:48+05:30

Activate Alternate Image | Cancel

1 In case the active firmware image is the alternate image, only the **Active Image** table is shown. In this case, the **Activate Alternate Image** button is also disabled.

2 If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.

3 The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

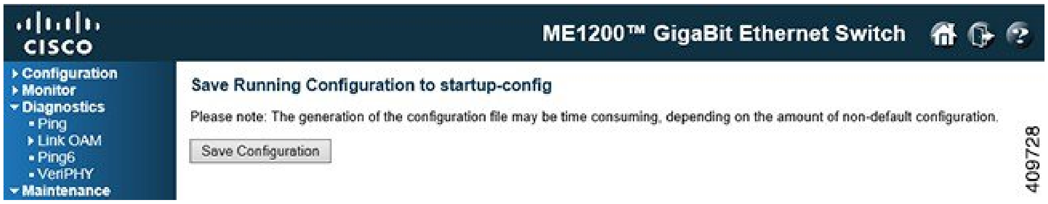
Image Information

- **Image**: The file name of the firmware image, from when the image was last updated.
- **Version**: The version of the firmware image.
- **Date**: The date where the firmware was produced.
- **Activate Alternate Image**: To use the alternate image, click **Activate Alternate Image**. This button may be disabled depending on system state.

Configuration

Maintaining Configuration Files

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch.



Save Running Configuration to startup-config

Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

The available files are:

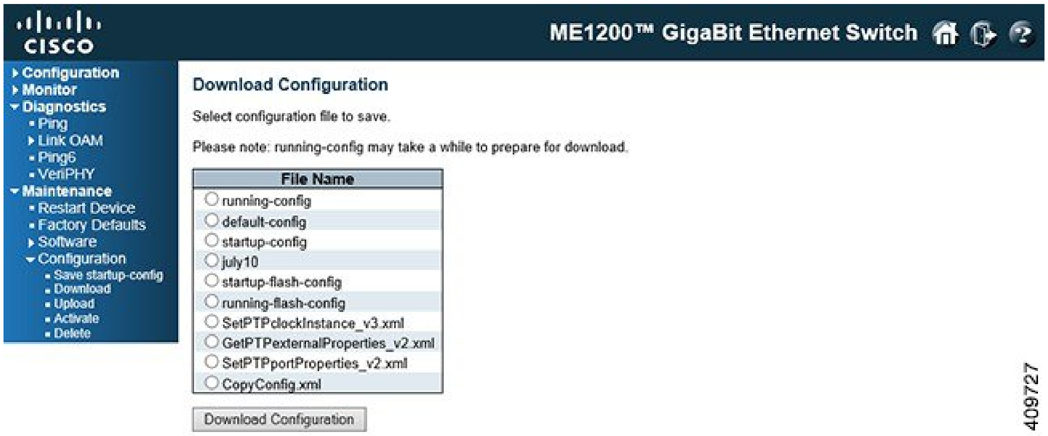
- *running-config*: A virtual file that represents the currently active configuration on the switch. This file is volatile.
- *startup-config*: The startup configuration for the switch, read at boot time. If this file does not exist at boot time, the switch will start up in default configuration.
- *default-config*: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.
- Up to 31 other files, typically used for configuration backups or alternative configurations.

Save *startup-config*

This option copies ***running-config*** to ***startup-config***, thereby ensuring that the currently active configuration will be used at the next reboot.

Download

It is possible to download any of the files on the switch to the web browser. Select the file and click **Download Configuration**.



Download Configuration

Select configuration file to save.

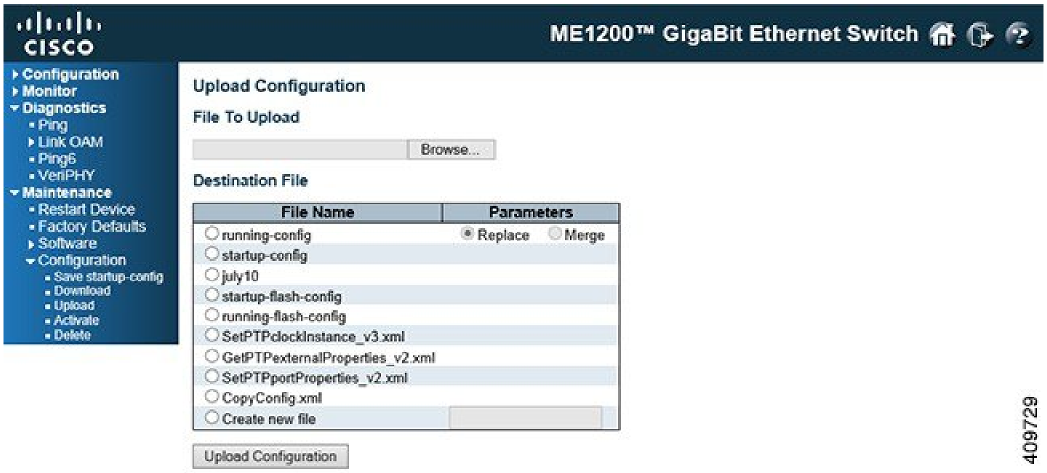
Please note: running-config may take a while to prepare for download.

File Name
○ running-config
○ default-config
○ startup-config
○ july10
○ startup-flash-config
○ running-flash-config
○ SetPTPclockInstance_v3.xml
○ GetPTPexternalProperties_v2.xml
○ SetPTPportProperties_v2.xml
○ CopyConfig.xml

Download of ***running-config*** may take a little while to complete, as the file must be prepared for download.

Upload:

It is possible to upload a file from the web browser to all the files on the switch, except default-config which is read-only. If the destination is running-config, the file will be applied to the switch configuration. This can be done in two ways:



Upload Configuration

File To Upload

Destination File

File Name	Parameters
○ running-config	● Replace ○ Merge
○ startup-config	
○ july10	
○ startup-flash-config	
○ running-flash-config	
○ SetPTPclockInstance_v3.xml	
○ GetPTPexternalProperties_v2.xml	
○ SetPTPportProperties_v2.xml	
○ CopyConfig.xml	
○ Create new file	

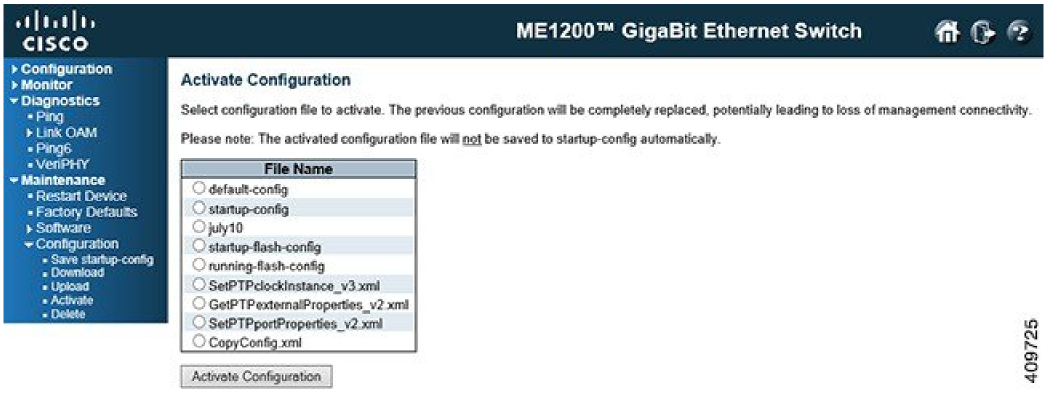
- **Replace mode**: The current configuration is fully replaced with the configuration in the uploaded file.
- **Merge mode**: The uploaded file is merged into *running-config*.

  If the flash file system is full (that is, contains default-config and 32 other files, usually including startup-config), it is not possible to create new files. Instead an existing file must be overwritten or another file must be deleted.

Select the file to upload, select the destination file on the target, then click **Upload Configuration**.

Activate

It is possible to activate any of the configuration files present on the switch, except for *running-config* which represents the currently active configuration.



Activate Configuration

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

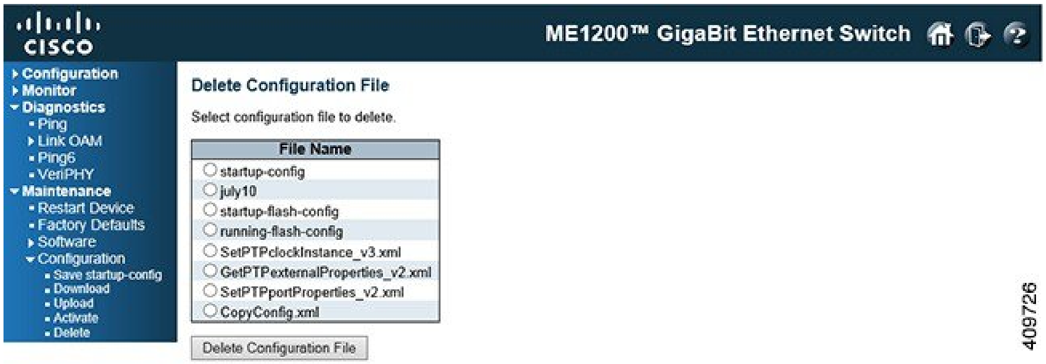
Please note: The activated configuration file will not be saved to startup-config automatically.

File Name
○ default-config
○ startup-config
○ july10
○ startup-flash-config
○ running-flash-config
○ SetPTPclockInstance_v3.xml
○ GetPTPexternalProperties_v2.xml
○ SetPTPportProperties_v2.xml
○ CopyConfig.xml

Select the file to activate and click **Activate Configuration**.

Delete

It is possible to delete any of the writable files stored in flash, including *startup-config*. If this is done and the switch is rebooted without a prior **Save** operation, this effectively resets the switch to default configuration.



Delete Configuration File

Select configuration file to delete.

File Name
○ startup-config
○ july10
○ startup-flash-config
○ running-flash-config
○ SetPTPclockInstance_v3.xml
○ GetPTPexternalProperties_v2.xml
○ SetPTPportProperties_v2.xml
○ CopyConfig.xml

Related Topics

Display and Save Configuration to FLASH, on page 3

CHAPTER 55

Use Cases

This section presents a few essential use cases for configuring in the ME 1200 Cisco Ethernet Switch Web GUI Interface.

Configuring Y.1731

This use case describes the flow of configurations that are required to configure the Y.1731 feature in the Cisco ME 1200 Web GUI Interface.

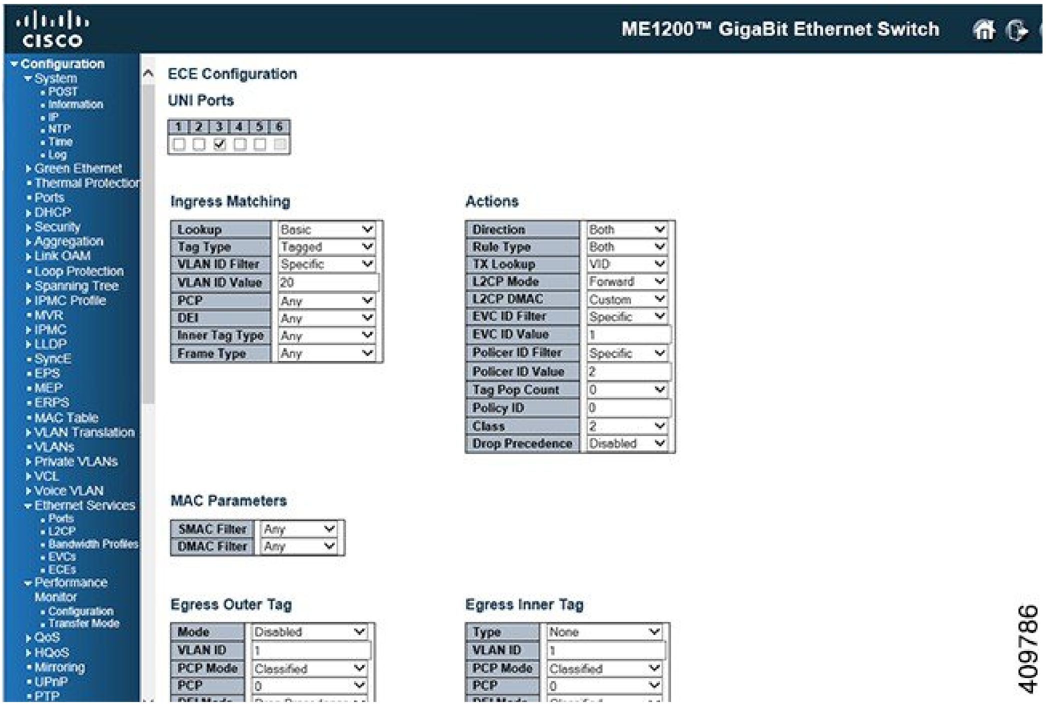
Prerequisites for ITU-T Y.1731 Performance Monitoring In a Service Provider Network

- IEEE-compliant Connectivity Fault Management (CFM) must be configured and enabled for Y.1731 performance monitoring to function.

Note If we are configuring MEP in EVC domain, EVC must be configured. If we are configuring MEP in VLAN domain, VLAN must be created.

Steps to Configure Y1731

Step 1 To configure ECE, click **Configurations** > **Ethernet Services** > **ECE**. For more information, ECE Control List Configuration, on page 108.



ECE Configuration

UNI Ports

1	2	3	4	5	6
□	□	☑	□	□	□

Ingress Matching

Lookup	Basic
Tag Type	Tagged
VLAN ID Filter	Specific
VLAN ID Value	20
PCP	Any
DEI	Any
Inner Tag Type	Any
Frame Type	Any

Actions

Direction	Both
Rule Type	Both
TX Lookup	VID
L2CP Mode	Forward
L2CP DMAC	Custom
EVC ID Filter	Specific
EVC ID Value	1
Policer ID Filter	Specific
Policer ID Value	2
Tag Pop Count	0
Policy ID	0
Class	2
Drop Precedence	Disabled

MAC Parameters

SMAC Filter	Any
DMAC Filter	Any

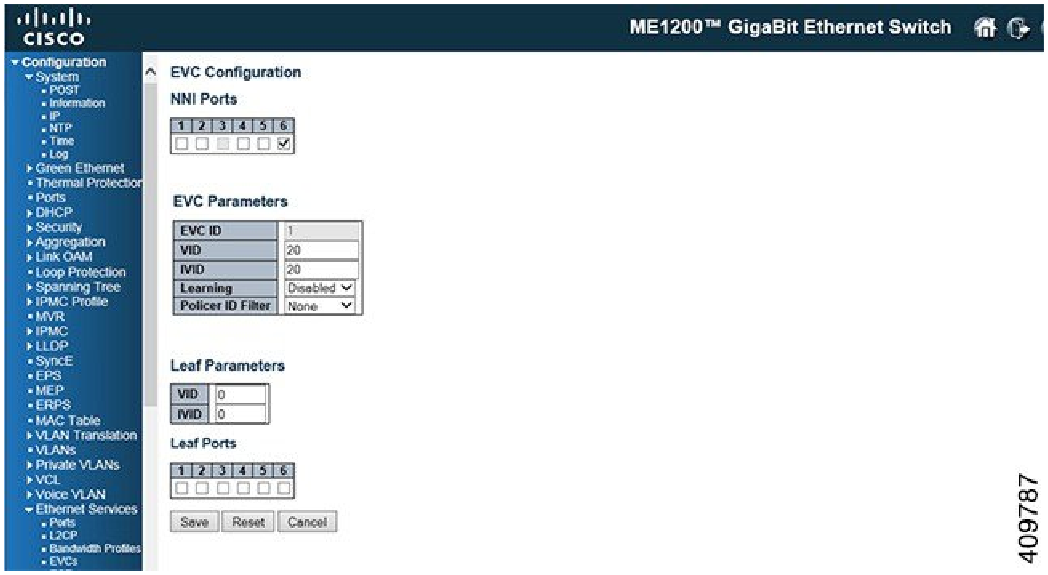
Egress Outer Tag

Mode	Disabled
VLAN ID	1
PCP Mode	Classified
PCP	0

Egress Inner Tag

Type	None
VLAN ID	1
PCP Mode	Classified
PCP	0

Step 2 To configure EVC, click **Configuration** > **Ethernet Services** > **EVCs**. For more information, see EVC Port Configuration, on page 103



EVC Configuration

NNI Ports

1	2	3	4	5	6
□	□	□	□	□	☑

EVC Parameters

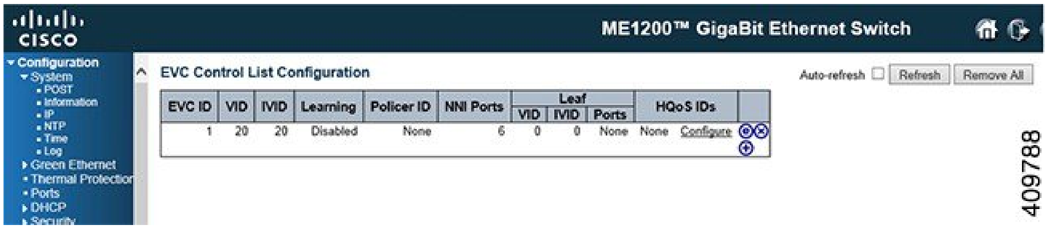
EVC ID	1
VID	20
IVID	20
Learning	Disabled
Policer ID Filter	None

Leaf Parameters

VID	0
IVID	0

Leaf Ports

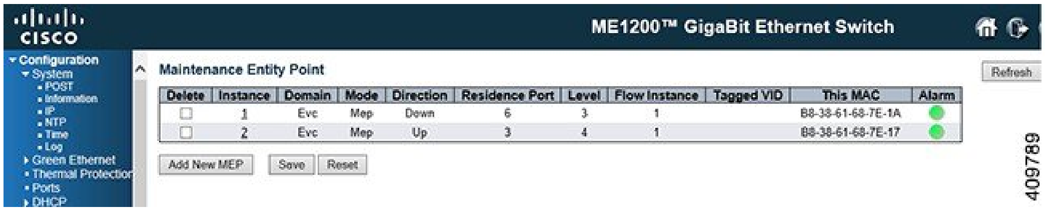
1	2	3	4	5	6
□	□	□	□	□	□



EVC Control List Configuration

EVC ID	VID	IVID	Learning	Policer ID	NNI Ports	Leaf			HQoS IDs	
						VID	IVID	Ports		
1	20	20	Disabled	None	6	0	0	None	None	Configure

Step 3 To configure MEP, click **Configuration** > **MEP**. For more information, see Maintenance Entity Point, on page 89

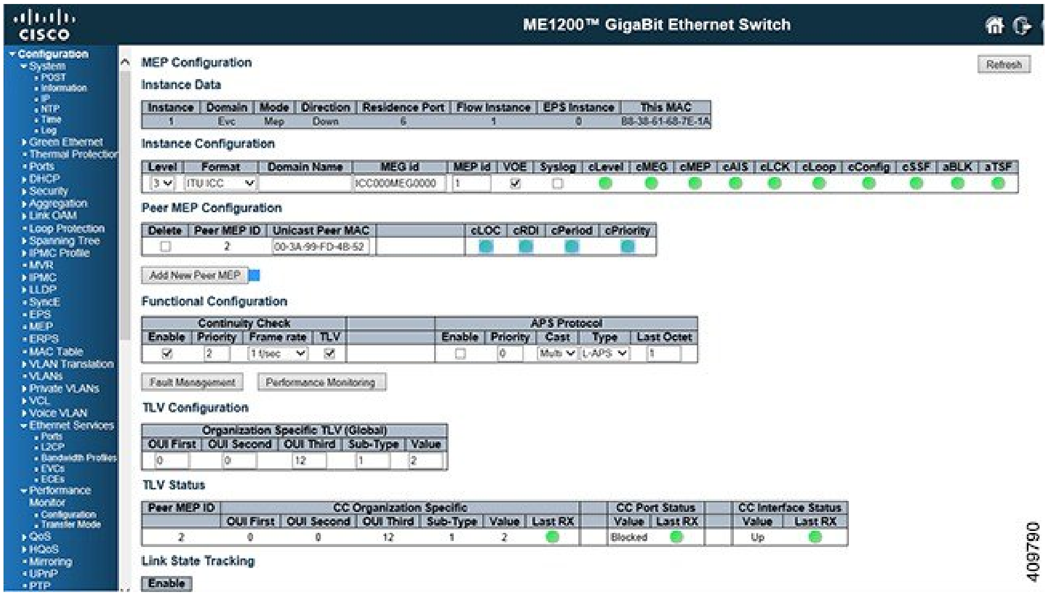


Maintenance Entity Point

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
□	1	Evc	Mep	Down	6	3	1		B8-38-61-68-7E-1A	●
□	2	Evc	Mep	Up	3	4	1		B8-38-61-68-7E-17	●

Add New MEP | Save | Reset

Step 4 Click on the instance number which is created in the above step to configure MEP parameters.



MEP Configuration

Instance Data

Instance	Domain	Mode	Direction	Residence Port	Flow Instance	EPS Instance	This MAC
1	Evc	Mep	Down	6	1	0	B8-38-61-68-7E-1A

Instance Configuration

Level	Format	Domain Name	MEG id	MEP id	VOE	Syslog	cLevel	cMEG	cMEP	cAIS	cLCK	cLoop	cConfig	cSSF	aBLK	aTSF
3	ITU ICC		ICC000MEG0000	1	☑	□	●	●	●	●	●	●	●	●	●	●

Peer MEP Configuration

Delete	Peer MEP ID	Unicast Peer MAC		cLOC	cRDI	cPeriod	cPriority
□	2	00-3A-99-FD-4B-52		●	●	●	●

Add New Peer MEP

Functional Configuration

Continuity Check					APS Protocol				
Enable	Priority	Frame rate	TLV		Enable	Priority	Cast	Type	Last Octet
☑	2	1 f/sec	☑		□	0	Multi	L-APS	1

Fault Management | Performance Monitoring

TLV Configuration

Organization Specific TLV (Global)				
OUI First	OUI Second	OUI Third	Sub-Type	Value
0	0	12	1	2

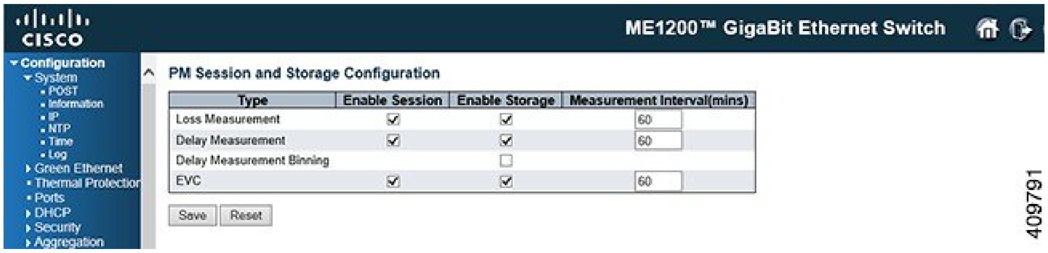
TLV Status

Peer MEP ID	CC Organization Specific							CC Port Status			CC Interface Status	
	OUI First	OUI Second	OUI Third	Sub-Type	Value	Last RX		Value	Last RX		Value	Last RX
2	0	0	12	1	2	●		Blocked	●		Up	●

Link State Tracking

Enable

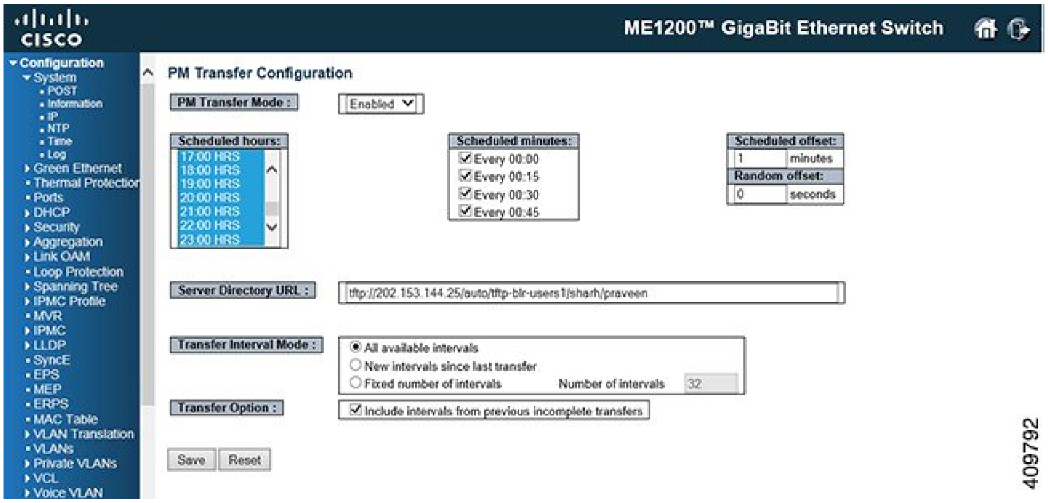
Step 5 To configure the Performance Monitoring session and storage, click **Configuration** > **Performance Monitor** > **Configuration**. This enables the session and storage parameters which stores session data in the RAM storage data in the flash respectively. For more information, see Performance Monitor Configuration, on page 111



PM Session and Storage Configuration

Type	Enable Session	Enable Storage	Measurement Interval(mins)
Loss Measurement	☑	☑	60
Delay Measurement	☑	☑	60
Delay Measurement Binning		☐	
EVC	☑	☑	60

Step 6 To transfer performance monitoring data to a tftp/http server, click **Configuration** > **Performance Monitor** > **Transfer Mode** . For more information, see Performance Monitor Transfer Configuration, on page 112



PM Transfer Configuration

PM Transfer Mode : Enabled

Scheduled hours: 17:00 HRS, 18:00 HRS, 19:00 HRS, 20:00 HRS, 21:00 HRS, 22:00 HRS, 23:00 HRS

Scheduled minutes: ☑ Every 00:00 ☑ Every 00:15 ☑ Every 00:30 ☑ Every 00:45

Scheduled offset: 1 minutes

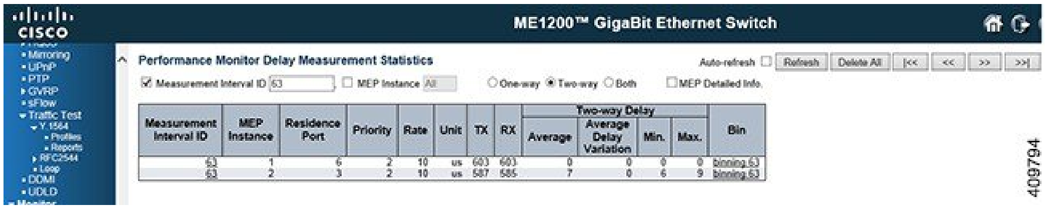
Random offset: 0 seconds

Server Directory URL : tftp://202.153.144.25/auto/tftp-blr-users1/sharh/praveen

Transfer Interval Mode : ● All available intervals ○ New intervals since last transfer ○ Fixed number of intervals Number of intervals 32

Transfer Option : ☑ Include intervals from previous incomplete transfers

Step 7 To enable Performance Monitoring, click **Configuration** > **MEP** > **MEP instance** > **Performance Monitoring**. For more information, see Maintenance Entity Point, on page 89



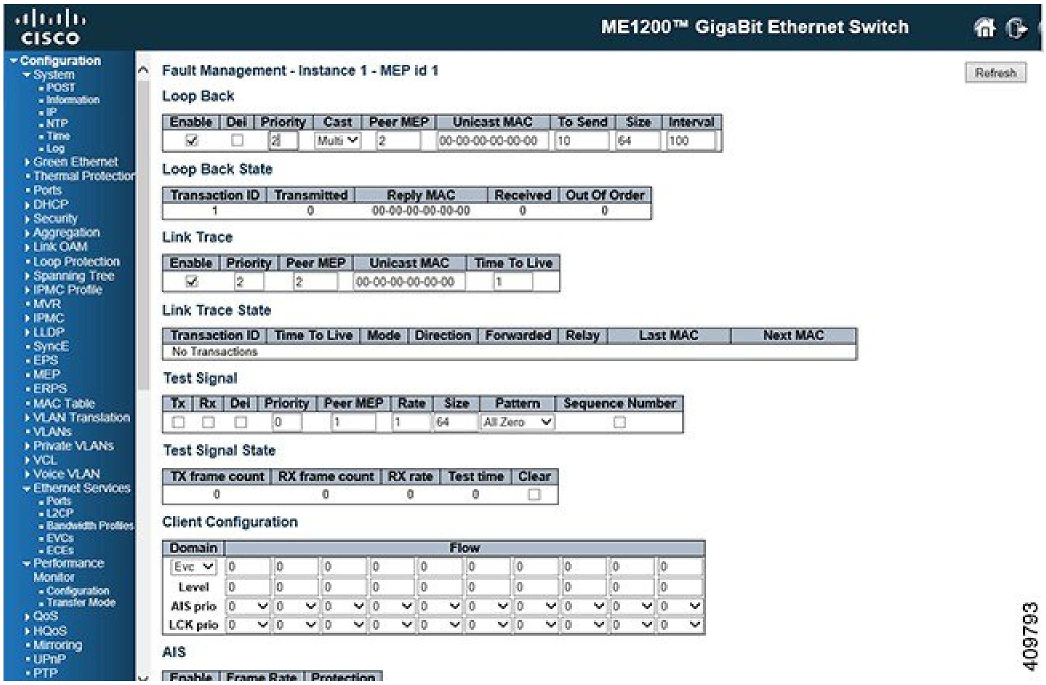
Performance Monitor Delay Measurement Statistics

Auto-refresh ☐

☑ Measurement Interval ID 63 ☐ MEP Instance All ○ One-way ● Two-way ○ Both ☐ MEP Detailed Info.

Measurement Interval ID	MEP Instance	Residence Port	Priority	Rate	Unit	TX	RX	Two-way Delay				Bin
								Average	Average Delay Variation	Min.	Max.	
63	1	6	2	10	us	603	603	0	0	0	0	binning.63
63	2	3	2	10	us	587	585	7	0	6	9	binning.63

Step 8 To enable Fault Management, click **Configuration** > **MEP** > **MEP instance** > **Fault Management.**For more information, see Maintenance Entity Point, on page 89



Fault Management - Instance 1 - MEP id 1

Loop Back

Enable	Dei	Priority	Cast	Peer MEP	Unicast MAC	To Send	Size	Interval
☑	□	2	Multi	2	00-00-00-00-00-00	10	64	100

Loop Back State

Transaction ID	Transmitted	Reply MAC	Received	Out Of Order
1	0	00-00-00-00-00-00	0	0

Link Trace

Enable	Priority	Peer MEP	Unicast MAC	Time To Live
☑	2	2	00-00-00-00-00-00	1

Link Trace State

Transaction ID	Time To Live	Mode	Direction	Forwarded	Relay	Last MAC	Next MAC
No Transactions							

Test Signal

Tx	Rx	Dei	Priority	Peer MEP	Rate	Size	Pattern	Sequence Number
□	□	□	0	1	1	64	All Zero	□

Test Signal State

TX frame count	RX frame count	RX rate	Test time	Clear
0	0	0	0	□

Client Configuration

Domain	Flow									
Evc	0	0	0	0	0	0	0	0	0	0
Level	0	0	0	0	0	0	0	0	0	0
AIS prio	0	0	0	0	0	0	0	0	0	0
LCK prio	0	0	0	0	0	0	0	0	0	0

AIS

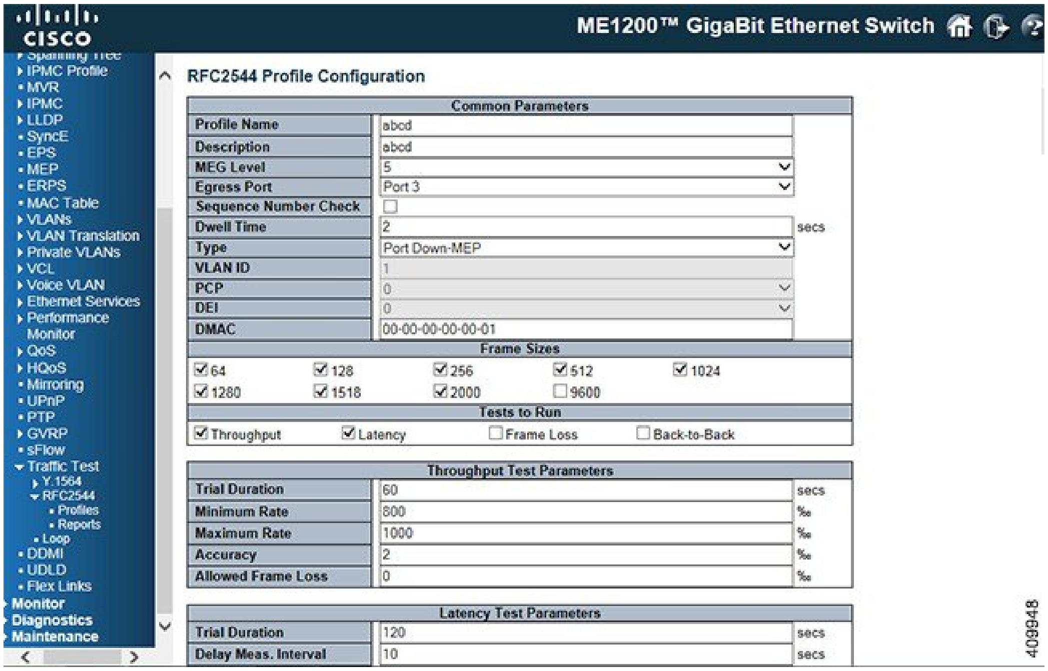
Enable	Frame Rate	Protection

Configuring RFC2544

This use case describes the flow of configurations that are required to configure the RFC2544 feature in the Cisco ME 1200 Web GUI Interface.

Steps to Configure RFC2544

Step 1 To configure RFC2544, click **Configuration** > **Traffic Test** > **RFC2544** > **Profiles**. This option provides an overview of the defined profiles along with options for editing and deleting them and creating new one. For more information, RFC2544 Profile Overview, on page 145



RFC2544 Profile Configuration

Common Parameters		
Profile Name	abcd	
Description	abcd	
MEG Level	5	
Egress Port	Port 3	
Sequence Number Check	□	
Dwell Time	2	secs
Type	Port Down-MEP	
VLAN ID	1	
PCP	0	
DEI	0	
DMAC	00-00-00-00-00-01	

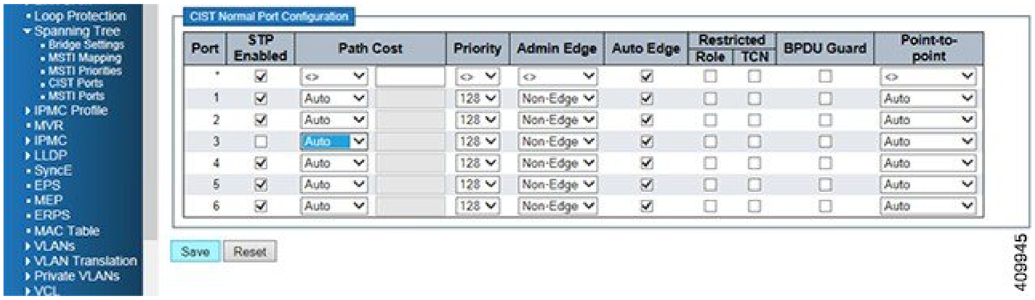
Frame Sizes				
☑ 64	☑ 128	☑ 256	☑ 512	☑ 1024
☑ 1280	☑ 1518	☑ 2000	□ 9600	

Tests to Run			
☑ Throughput	☑ Latency	□ Frame Loss	□ Back-to-Back

Throughput Test Parameters		
Trial Duration	60	secs
Minimum Rate	800	‰
Maximum Rate	1000	‰
Accuracy	2	‰
Allowed Frame Loss	0	‰

Latency Test Parameters		
Trial Duration	120	secs
Delay Meas. Interval	10	secs

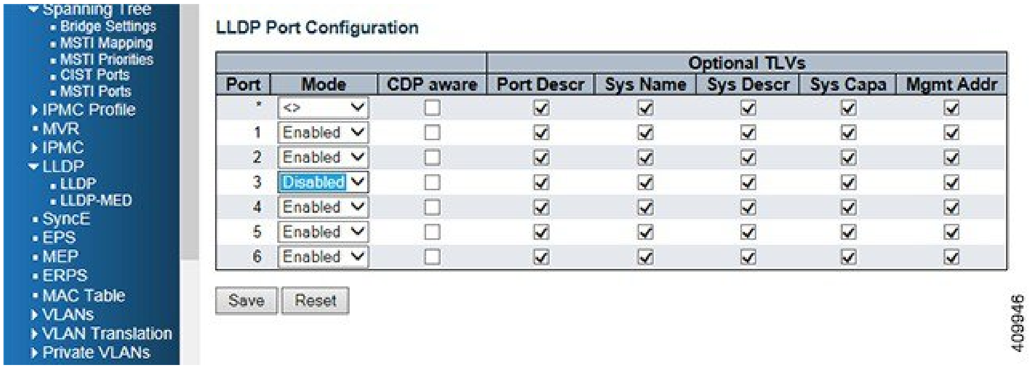
Step 2 To disable Port 3 in STP, click **Configuration** > **Spanning Tree** > **CIST Ports**. The STP option allows you to inspect the current STP CIST port configurations and change them. For more information, see STP CIST Port Configuration, on page 68



CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
*	☑	<>		<>	<>	☑	□	□	□	<>
1	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
2	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
3	□	Auto		128	Non-Edge	☑	□	□	□	Auto
4	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
5	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
6	☑	Auto		128	Non-Edge	☑	□	□	□	Auto

Step 3 To disable LLDP on Port 3, click **Configuration** > **LLDP** > **LLDP Port Configuration**. The LLDP option allows you to inspect and configure the current LLDP port settings. For more information, see LLDP Configuration, on page 75

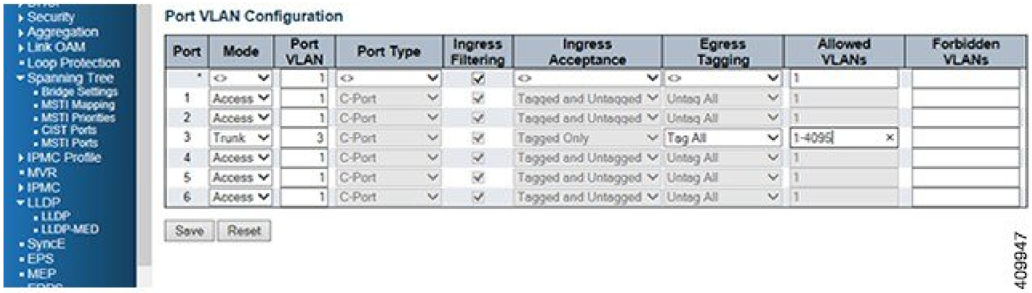


LLDP Port Configuration

			Optional TLVs				
Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	□	☑	☑	☑	☑	☑
1	Enabled	□	☑	☑	☑	☑	☑
2	Enabled	□	☑	☑	☑	☑	☑
3	Disabled	□	☑	☑	☑	☑	☑
4	Enabled	□	☑	☑	☑	☑	☑
5	Enabled	□	☑	☑	☑	☑	☑
6	Enabled	□	☑	☑	☑	☑	☑

Save Reset

Step 4 To configure VLAN settings, click **Configuration** > **VLAN** > **VLAN Configuration**. For more information on configuring VLANs, see VLAN Configuration, on page 97

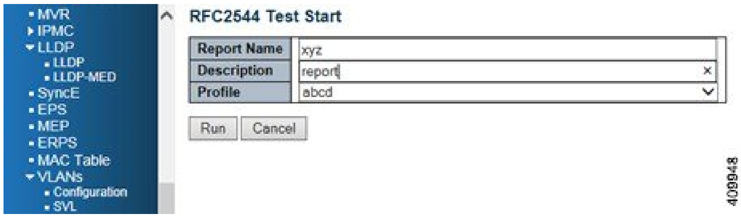


Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Trunk	3	C-Port	☑	Tagged Only	Tag All	1-4095	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Save Reset

Step 5 To execute a test run of RFC2455 configuration, click **Configuration** > **Traffic Test** > **RFC2544** > **Reports**. For more information, see RFC2544 Report Overview, on page 146

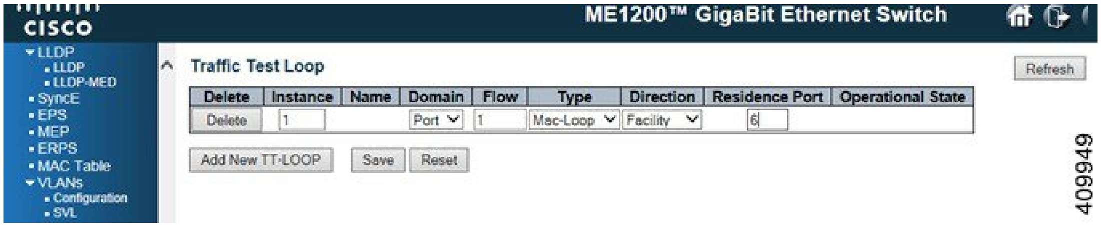


RFC2544 Test Start

Report Name	xyz
Description	report
Profile	abcd

Run Cancel

Step 6 To configure on a remote nid to Loop, click **Configuration** > **Traffic Test** > **RFC2544** > **Loop**. For more information, see TT-LOOP, on page 146

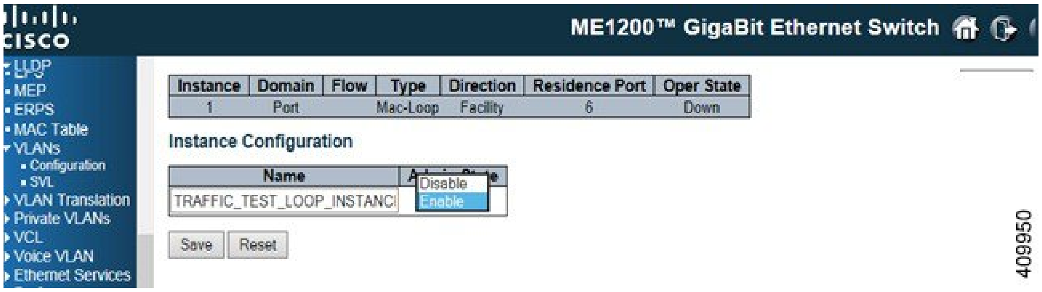


Traffic Test Loop

Delete	Instance	Name	Domain	Flow	Type	Direction	Residence Port	Operational State
Delete	1		Port	1	Mac-Loop	Facility	6	

Add New TT-LOOP Save Reset

Step 7 The loopback must be enabled in the remote end and port should be *Active*. For more information, see Maintenance Entity Point, on page 89



Instance	Domain	Flow	Type	Direction	Residence Port	Oper State
1	Port		Mac-Loop	Facility	6	Down

Instance Configuration

Name	Admin State
TRAFFIC_TEST_LOOP_INSTANC	Disable [✓ Enable]