Cisco ME1200 iCLI Configuration Guide

First Published: August 5, 2016
Last Updated: May, 2018

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

Text Part Number: NA

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2016-2018 Cisco Systems, Inc. All rights reserved.

CHAPTER 1

ICLI Configuration

This document describes basic usage and configuration of the Industrial Command Line Interface (ICLI). The ICLI is a comprehensive management interface to the device. It is the only management interface accessible on the serial console; even without network connectivity, the device can be managed using a serial connection.

Quick Start

This section describes how to perform the following:

- Log in and reset configuration to factory defaults
- Set device hostname and admin user password
- Set VLAN 1 IP address
- Verify connectivity using ‘ping’
- Display the current configuration and save it to flash storage

The following assumes the 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).

The computer must be running a terminal emulator such as TeraTerm or PuTTY on Windows, or Minicom on Linux.

Log In and Reset Configuration to Factory Default

Press **Enter** one or more times until the Username: prompt appears. Type **admin** and press **Enter**. At the Password: prompt type **sandino** and press Enter. This completes the login sequence and displays the prompt, ‘#’.

```
Username: admin
Password:
#
```

At this point, the admin user is operating at the highest privilege level, level 15. This means full control over the device and its configuration, and it is therefore possible to reset the configuration to factory defaults. Type **reload defaults** and press **Enter**. When the prompt returns, the system has reverted to factory defaults as follows.

```
# reload defaults
% Reloading defaults. Please stand by.
#
```

Set Device Hostname and Admin User Password

The ICLI has several different modes. The current mode is called *exec* mode; it allows the user to perform operations related to configuration files, reloading defaults, displaying system information, etc., but it does not allow the user to change detailed configuration items. Such operations are performed while in the *config mode*.

To set the device hostname, first change to configuration mode by typing **configure terminal** and press **Enter**, then type **hostname my-device** and press **Enter**, where **my-device** is a suitable name for the device. Finally, type **exit** and press **Enter**. The sequence should appear as shown here.

```
# configure terminal
(config)# hostname my-device
my-device(config)# exit
my-device#
```

The commands are executed immediately, so `hostname` changes the device hostname right away. A password should be set for the admin user.

```
my-device# configure terminal
my-device(config)# username admin privilege 15 password unencrypted
very-secret
my-device(config)# exit
my-device#
```

The user, admin, now has the password “very-secret.” Other users can be added in similar fashion.

Set VLAN 1 IP Address

The objective is to assign an IP address to the device on VLAN 1. This is often sufficient for small local area networks that use Dynamic Host Configuration Protocol (DHCP) or static IP address allocation.

The system implements a DHCP client that, once enabled, will send out requests for IP address configuration. Those requests are received by a DHCP server on the network (if present and appropriately configured). The server will then search through its pool of available IP addresses, allocate one, and return it to the DHCP client. The returned information typically includes IP address, netmask, and default gateway, but may also contain other information such as Domain Name Service (DNS) server addresses.

The configuration proceeds in the same manner as setting the hostname: Enter configuration mode, input and execute configuration commands, leave configuration mode. The following commands instruct the device to use DHCP to obtain an IP address, or, if DHCP fails, to use a static fallback address. Inclusion of a fallback IP is optional and may be omitted.

```
my-device# configure terminal
my-device(config)# interface vlan 1
my-device(config-if-vlan)# ip address dhcp fallback 172.16.1.2
255.255.0.0
my-device(config-if-vlan)# exit
my-device(config)#
```

Notice how the prompt changes; the `interface vlan 1` command enters a configuration *sub-mode* that allows, among other things, configuration of IP address.

Also note that IP addresses can only be assigned to *VLAN interfaces*.

After configuration is complete, the resulting IP address can be inspected. As seen below, the DHCP negotiation succeeded and the device obtained an address:

```
my-device# show ip interface brief
Vlan Address Method Status
---- -------------------- -------- ------
1 172.16.1.17/16 DHCP UP
my-device#
```

`show ip interface brief` displays all configured and active IP interfaces. The status should be UP. If it isn't, then the reason could be that there is no link on any port.

If DHCP negotiation failed then the fallback IP of 172.16.1.2/255.255.0.0 would be assigned.

Now the most basic system configuration is complete. Management connectivity can be verified by issuing a `ping` command to a well-known external IP address:

```
my-device# ping ip 172.16.1.1
PING server 172.16.1.1, 56 bytes of data.
64 bytes from 172.16.1.1: icmp_seq=0, time=0ms
64 bytes from 172.16.1.1: icmp_seq=1, time=0ms
64 bytes from 172.16.1.1: icmp_seq=2, time=0ms
64 bytes from 172.16.1.1: icmp_seq=3, time=0ms
64 bytes from 172.16.1.1: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
my-device#
```

If the ping is successful, network logins can now be performed through *telnet* or *ssh* to the address on VLAN interface 1, 172.16.1.17 (or 172.16.1.2).

Display and Save Configuration to Flash

The current configuration of the device can be displayed in the form of a virtual file containing the full set of commands necessary to create an identical configuration. A few exceptions exist because certain items are not displayed, such as private SSH keys. This file is called *running-config* and is volatile by nature; it does not survive across reboots. It is therefore necessary to save the file to flash storage under the name *startup-config*, as this file is read and executed upon every boot and is therefore responsible for restoring the running configuration of the system to the state it had when the save took place.

The command `show running-config` will display the configuration settings as seen below. For brevity, some details were edited out. In addition, the set of interfaces is dependent on hardware capabilities.

```
my-device# show running-config
Building configuration...
hostname my-device
username admin privilege 15 password encrypted
3ad61dc090116a16a7cc9861485e60e6407c5a328015b1985b585ab353c37a4441e034
172401528229795a5c9529dfbc04c86e01
!
vlan 1,42
!
spanning-tree mst name 00-01-c1-00-ad-80 revision 0
! [...]
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
! [...]
!
interface GigabitEthernet 1/1
```

```
!
interface GigabitEthernet 1/2
!
interface vlan 1
ip address dhcp fallback 172.16.1.2 255.255.0.0
!
line console 0
!
line vty 0
!
! [...]
!
end
my-device#
```

Lines that begin with ‘!’ are comments. The file begins with the `hostname` command and the password for the admin user, followed by VLANs 1 and 42 and other items, such as Spanning Tree Protocol (STP). A list of all port interfaces on the device, ordered by switch ID, type, and port number comes next.

All port interfaces are at default settings, so nothing is displayed for them. As a general rule, only non-default configuration is displayed, otherwise the output would be huge and readability would suffer. There are a few exceptions that will be discussed later.

Following the physical interfaces are VLAN interfaces 1 and 42. Only the former has an IP address assigned. Finally, the line section is shown. It specifies characteristics for the serial console (line console 0) or network ICLI management connections (line vty *x*).

The configuration as displayed above is also what is saved to *startup-config.*

```
my-device# copy running-config startup-config
Building configuration...
% Saving 1326 bytes to flash:startup-config
my-device# dir
Directory of flash:
r- 1970-01-01 00:00:00 648 default-config
rw 1970-01-03 18:21:28 1326 startup-config
2 files, 1974 bytes total.
my-device# more flash:startup-config
hostname my-device
username admin privilege 15 password encrypted
3ad61dc090116a16a7cc9861485e60e6407c5a328015b1985b585ab353c37a4441e034
172401528229795a5c9529dfbc04c86e01
!
vlan 1,42
[...]
```

The `dir` command lists the files in the flash file system while `more` outputs the contents of the designated file.

The skills exercised in this section form the basis for all day-to-day work with the ICLI on the device: logging in, displaying information with the `show` command, working with configuration files (`show running-config`, `copy`, `dir`, `more`), working with the actual configuration (`configure terminal`, `exit`), and sub-modes (`interface ...`).

The configuration proceeds in the same manner as setting the hostname: Enter configuration mode, input and execute configuration commands, leave configuration mode. The following commands instruct the device to use DHCP to obtain an IP address, or, if DHCP fails, to use a static fallback address. Inclusion of a fallback IP is optional and may be omitted.

ICLI Basics

The following list shows the key ICLI characteristics:

- It is modal (certain operations are possible or impossible in specific modes)
- It is line-based (there are no screen editing features)
- It executes commands instantly upon end-of-line
- It is privilege-based (certain operations require the user to have a certain privilege level to succeed)
- It implements industrial de-facto behavior for network equipment CLIs (structurally and behaviorally, it resembles CLIs found on other equipment while still possessing unique characteristics in some areas)

The ICLI can be accessed directly using the serial console, or over the network through *telnet* or *ssh.* In each case, the user has to log in before ICLI commands can be executed. This begins a *session* that lasts until logout.

Multiple sessions can co-exist at the same time, each providing separate environments: logged-in user ID, privilege level, command history, mode, and session settings. It is therefore perfectly possible for the same user to control several concurrent sessions, such as one serial console session and one ssh session.

The user database is either local or provided by a RADIUS or TACACS+ server. In case of a local user database, passwords and privilege levels are maintained on the device.

Command Structure and Syntax

A *command* is a single line of text consisting of keywords and parameters, for example:

```
my-device# show vlan id 10
...
my-device# show vlan id 20
...
```

The keywords are `show, vlan,` and `id;` whereas 10 and 20 are parameters, something that could contain another value in another command invocation.

Keywords are not case sensitive, thus `show`, `SHOW`, and `Show` are identical. Conversely, parameters may either be case-sensitive or not, depending on the command and parameter in question.

Keywords and certain parameters can be abbreviated as long as they are unambiguous. For example, these commands are identical:

```
my-device# show interface GigabitEthernet 1/5 capabilities
...
my-device# sh int g 1/5 c
...
```

This works because:

- There are many keywords that begin with ‘s’ but only one that begins with ‘sh’
- There are several commands that begin with ‘show i’ but only one that begins with ‘show in’
- The `show interface` command takes a port type as parameter. Depending on the hardware capabilities, the options are: FastEthernet, GigabitEthernet, Thus, ‘g’ is a unique abbreviation for GigabitEthernet
- 1/5 identifies the interface as belonging to switch 1, port 5. This parameter cannot be abbreviated and has to be written out in full
- The `show interface GigabitEthernet 1/5` command can output different kinds of information: Capabilities, statistics, status, and several other. In this case, ‘c’ is a unique abbreviation for capabilities

With a bit of practice, this allows for highly efficient keyboard entry, in particular when coupled with the context-sensitive help features of the ICLI (see Context-Sensitive Help).

Syntax

A command is described by its syntax, for example:

```
show interface { * | GigabitEthernet | vlan}
```

and

```
show erps [ groups ] [ detail | statistics ]
```

```
my_device# show interface ?

* All switches or all ports
GigabitEthernet 1 GigabitEthernet Port
vlan VLAN Status
```

Note Syntax is represented in a slightly different manner in this documentation as compared to a ICLI session. In this document, variable parameters are written in *italics*, whereas a ICLI session will display such items surrounded by '<' and '>'.

The semantics are:

- **keywords** are written in bold
- *parameters* are written in italics
- [...] indicates an optional construct: It may or may not be present
- { ... } indicates a grouping; the constructs within belong together
- '|' indicates a choice between two or more alternatives, (example, **a | b | c** which reads as "a or b or c").

Thus, the first command syntax is simple: First `show`, then `interface`, then a list of interfaces, then exactly one of `status`, `statistics`, `capabilities`, `switchport`, and `veriphy`.

The second command is a bit more complex: `show` and `erps` are mandatory, but the remaining parameters and keywords are optional: The user may enter group IDs; the user may enter either 'statistics' or 'detail'. For example:

```
! Show short-form ERPS (Ethernet Ring Protection Switching) information
for all
! instances:
my-device# show erps
...
! Show statistics for all instances:
my-device# show erps statistics
...
! Show details for all instances:
my-device# show erps detail
...
! But it is not allowed to show details and statistics at the same time:
my-device# show erps detail statistics
                            ^
% Invalid word detected at '^' marker.
! Show details for specific set of instances:
my-device# show erps 1-6 detail
...
```

There are some slightly more complex features of the syntax that center around sequences of optional items such as `[a] [b] [c]`.

- Each of a, b, c may or may not be present (“a c” is valid, as is no input)
- Order is not important (“a c” and “c a” are equivalent)
- Each optional item can be present exactly no times or one time (not repeated)

There are variations:

- Group of options, of which at least one must be present: `{  [a] [b] [c] }*1`
- Group of options, where one or more has fixed position: `[a] {[b]} [c]`
- This says that ‘b’ is optional, but if it is present then it must follow after ‘a’ (if ‘a’ is present) and it must come before ‘c’ (if ‘c’ is present)

For example, assuming a command with this syntax:

```
a [b] [c] { d | e } {[f] [g]}*1
```

then valid input examples are:

- ‘a d f’, because ‘b’ and ‘c’ are optional, ‘d’ is picked instead of ‘e’, and ‘f’ is chosen as the mandatory optional
- ‘a d f g’, because ‘b’ and ‘c’ are optional, ‘d’ is picked instead of ‘e’, and both ‘f’ and ‘g’ are chosen in the final group of optional
- ‘a c b e g’, because the ‘b’ optional is omitted, ‘e’ is picked instead of ‘d’, and ‘g’ is chosen for the mandatory optional

Ethernet Interface Naming

An Ethernet interface, or port, is identified by three pieces of information:

- The type (FastEthernet, GigabitEthernet)
- The switch it belongs to (for non-stacking systems, this value is always 1)
- The port number within the type and switch (numbering starts with 1 for each type, so a switch may have both `GigabitEthernet 1/1)`

Many ICLI commands accept a list of interfaces. In its simplest form, such a list is a sequence of (type, switch ID, port) information separated by whitespace. For example: `GigabitEthernet 1/3 10GigabitEthernet 1/2.` This allows a single list to mix different types.

The switch ID and the port numbers can be listed either as single numbers, as lists, or as sequences. A list is a comma-separated set of single port numbers or sequences, whereas a sequence is of the form: *from—to.*

Some examples:

- GigabitEthernet 1/5 for the single gigabit port number 5 on switch 1
- GigabitEthernet 1/2,4,10-12 for gigabit ports 2, 4, 10, 11, 12 on switch 1
- GigabitEthernet 1-3/2 for gigabit port 2 on switches 1, 2 and 3

It is possible to *wildcard* the type and/or switch ID and/or ports to mean “all types,” “all switch IDs,” and “all ports,” respectively. A wildcard is written with an asterisk instead of type, switch ID, or port, and some further abbreviations are possible:

- ‘*’ means “all ports of all types on all switches”
- *type* ‘*’ means “all ports of the specified type on all switches”

To clarify, several examples are provided. Assume a stack with two switches, switch ID 1 and 3. Each switch has 6 gigabit ports. Then:

- interface * (or: interface * * *)
  - All ports of all types on all switches: GigabitEthernet 1,3/1-9
- interface * 1/2
  - Switch 1, port number 2 of all types: GigabitEthernet 1/2
- interface * */2

    - All switches, all types, port number 2: GigabitEthernet 1,3/2
- interface * */4
    - All switches, all types, port number 4: GigabitEthernet 1,3/4

There are no 2.5 gigabit ports in the result.

- interface GigabitEthernet 3/*
    - Switch 3, all gigabit ports: GigabitEthernet 3/1-9

Wildcards will include the largest possible set of ports, but may output an error message if a specific switch ID or port number doesn’t exist.

For example, these sets are invalid:

- interface * 2/*
    - All ports of all types on switch 2 – which isn’t a member of the stack
- interface * */100
    - There is no port 100 of any type on any switch
- interface GigabitEthernet */*
    - Again, switch 2 doesn’t exist so the entire set is considered invalid

Validity is determined per set of (type, switch ID, port) containing wildcards: The result for that set is valid if there is at least one port that matches the set. A list of sets is valid if all sets match at least one port each.

Using the Keyboard

The ICLI provides a rich set of keys to assist the user while working with the command line. The functionality is divided into:

- Basic line editing
- Command history
- Context-sensitive help
- Long lines and pagination

Basic Line Editing

Basic line editing allows the input of characters to form a command line, while also allowing cursor movement and insertion/deletion of characters and words. The following table shows the available editing functions and keys.

Table 1 • **Basic Line Editing Key**

Key	Operation
Left/Right	Move one character left/right
Home/Ctrl-A	Move to start of line
End/Ctrl-E	Move to end of line
Del/Ctrl-D	Delete character at cursor
Backspace/Ctrl-H	Delete character to the left of cursor
Ctrl-N	Delete the entire current line
Ctrl-U/Ctrl-X	Delete all characters to the left of the cursor
Ctrl-K	Delete all characters under the cursor and right
Ctrl-W	Delete from cursor to start of word on the left
TAB	Complete word at end-of-line

Command History

A session maintains a non-persistent command history of previously entered command lines. The history can be up to 32 lines long. Once full, a new line will push the oldest entry out.

Table 2 • **Command History**

Key	Operation
Up/Ctrl-P	Previous line in command history
Down	Next line in command history

The number of lines to keep in the history for the current session is configurable between 0 and 32, where 0 disables the history altogether.

```
my-device# terminal history size 32
```

The current value is displayed as part of the output from `show terminal`:

```
my-device# show terminal
Line is con 0.
    * You are at this line now.
    Alive from Console.
    Default privileged level is 2.
    Command line editing is enabled
    Display EXEC banner is enabled.
    Display Day banner is enabled.
    Terminal width is 80.
             length is 24.
             history size is 32.
             exec-timeout is 10 min 0 second.
    Current session privilege is 15.
    Elapsed time is 0 day 0 hour 6 min 20 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.
```

It is possible to list the history:

```
my-device# show history
  show running-config
  copy running-config startup-config
  dir
  show history
my-device#
```

The list begins with the oldest entry at top.

Context-Sensitive Help

The ICLI implements several hundred commands ranging from the very simple to the very complex. It is therefore imperative that the user can be assisted in entering syntactically correct commands as well as discovering relevant commands. These objectives are supported by the context sensitive help features.

Table 3 • **Context-Sensitive Help**

Key	Operation
?	Show next possible input and description

Table 3 • **Context-Sensitive Help**

Key	Operation
??/Ctrl-Q	Show syntax of possible command(s)
TAB	Show next possible input without description or expand current word if it is unambiguous

The context-sensitive help only displays commands that are accessible at the current session privilege level (see Understanding Privilege Levels, page 1-16).

Using Context-Sensitive Help

```
! Show possible next input for a command that begins with 'show a':
my-device# show a?
    aaa            Login methods
    access         Access management
    access-list    Access list
    aggregation    Aggregation port configuration

! The same, but without descriptions:
my-device# show a<TAB>
aaa        access       access-list  aggregation
! If the user enters another 'g' the word 'aggregation' is the only
possibility:
my-device# show ag?
    aggregation    Aggregation port configuration
    <cr>
! Pressing <TAB> now expands the word fully:
my-device# show aggregation
! Possible next input is displayed with a press of '?':
my-device# show aggregation ?
    |       Output modifiers
    mode    Traffic distribution mode
    <cr>
! The syntax is displayed with another press of '?':
my-device# show aggregation ?
show aggregation [ mode ]
! This shows that there is an optional 'mode' word (square brackets
indicate an option).
! Repeated presses of '?' toggles display between next possible input
and syntax:
my-device# show aggregation ?
    |       Output modifiers
    mode    Traffic distribution mode
    <cr>
my-device# show aggregation ?
show aggregation [ mode ]
! Finally, the syntax display is also directly available with Ctrl-Q:
my-device# show aggregation ^Q
show aggregation [ mode ]
```

Long Lines and Pagination

A session has a configuration that indicates the width of the terminal in characters and the length in lines. It uses these parameters to control handling of long input lines and to control pagination of multi-line output. For details about changing these parameters, see Understanding

Terminal Parameters, page 1-17.

Long lines come into play when a line is longer than the terminal width minus the prompt. In that case, part of the line will be hidden from display as indicated by '$' at the beginning and/or end of the visible part of the line.

For example:

```
my-device# $there is text to the left of what is visible here
my-device# there is text to the right of what is visible here$
my-device# $there is text at both ends of what is visible here$
```

The first line has scrolled left; the second line has scrolled right; the third line has been scrolled to the middle of a quite long line.

Pagination appears each time execution of a command causes output of more lines than what has been configured as the terminal length. A typical example is the output from `show running-config`. After the first several lines have been output, the pagination prompt is presented:

```
! [lines of text]
-- more --, next page: Space, continue: g, quit: ^C
```

The following keys control pagination:

Table 4 • **Pagination Keys**

Key	Operation
Enter	Display next line of output
Space	Display next page of output
G	Display remainder of output without more pagination
Q/Ctrl-C	Display remainder of output
Any other key	Display next page of output. Certain terminal keys (arrows, Home, End, etc.) may appear as multiple characters to the ICLI, leading to multiple pages being output in quick succession.

The terminal length (also sometimes called height) can be configured for the current session using the `terminal length` *lines* command. If *lines* = 0 is input, pagination is disabled.

```
my-device# terminal length 0
my-device# terminal length 25
```

The same is true for setting the terminal width in characters.

Other Special Keys

One additional key is defined as a convenience. It allows the immediate return from any sub-mode to Exec mode.

Table 5 • **Special Keys**

Key	Operation
Ctrl-Z	Return directly to Exec mode

Filtering Output

The output from commands can be filtered in most cases. It is possible to limit the output to only those lines that match/trigger a specific substring. The available filtering is:

- Begin – display the first line that matches and all subsequent lines
- Include – display exactly those lines that match
- Exclude – display exactly those lines that do not match

The string is case-sensitive.

The syntax is:

command ‘|’ { `begin` **|** **`include`** **|** **`exclude`** } *string*

```
! Execute a command that generates some output; no filtering initially:
my-device# show users
Line is con 0.
    * You are at this line now.
    Connection is from Console.
    User name is admin.
    Privilege is 15.
    Elapsed time is 0 day 21 hour 52 min 50 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.
! Filter to include specific word:
my-device# show users | include User
    User name is admin.
! Exclude all lines that contain ‘0’ (zero)
my-device# show users | exclude 0
    * You are at this line now.
    Connection is from Console.
    User name is admin.
    Privilege is 15.
! Begin output when specific word is matched:
my-device# show users | begin Elapsed
    Elapsed time is 0 day 21 hour 53 min 29 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.
```

Understanding Modes and Sub-Modes

The ICLI implements a number of modes that control the available command set. The modes are further influenced by the privilege level of the user; some modes or commands are only accessible to administrators while others require no privileges beyond login.

There are three major modes: Exec, Privileged Exec, and Config. Under Config, there exist a number of sub-modes. The sub-modes allow configuration of specific VLANs, Ethernet interfaces, etc.

Table 6 • **Modes**

Mode	Parent Mode	Description
Exec		Lowest-privileged mode; used for basic system monitoring. Generally does not allow modifications to the system Command: `disable` Prompt: `hostname>`
Privileged Exec	Exec	Privileged mode; allows configuration and other modifications to the system Command: `enable` Prompt: `hostname#`
Config	Priv.Exec	Global configuration mode Command: `configure terminal` Prompt: `hostname(config)#`
VLAN Config	Config	Sub-mode for configuring active VLANs Command: `vlan vlan_id_list` Prompt: `hostname(config-vlan)#`
VLAN Interface Config	Config	Sub-mode for configuring VLAN interfaces Command: `interface vlan vlan_id_list` Prompt: `hostname(config-if-vlan)#`
Interface Config	Config	Sub-mode for configuring Ethernet interfaces Command: `interface type switch_num/port_num` Prompt: `hostname(config-if)#`
Line	Config	Sub-mode for configuring terminal lines Command: `line { con | vty } line_num` Prompt: `hostname(config-line)#`
IPMC Profile Config	Config	Sub-mode for configuring IP Multicast profiles Command: `ipmc profile profile_name` Prompt: `hostname(config-ipmc-profile)#`
SNMP Server Host Config	Config	Sub-mode for configuring SNMP server host entries Command: `snmp-server host host_name` Prompt: `hostname(config-snmps-host)#`
STP Aggregation Config	Config	Sub-mode for configuring Spanning Tree Protocol aggregation Command: `spanning-tree aggregation` Prompt: `hostname(config-stp-aggr)#`
DHCP Pool Config	Config	Sub-mode for configuring DHCP client pools Command: `ip dhcp pool pool_name` Prompt: `hostname(config-dhcp-pool)#`
RFC2544 Profile Config	Config	Sub-mode for configuring RFC2544 profiles Command: `rfc2544 profile profile_name` Prompt: `hostname(config-rfc2544-profile)#`

Table 6 • **Modes (continued)**

Mode	Parent Mode	Description
Y.1564 Config	Config	Sub-mode for configuring Y.1564 profiles Command: `y1564 profile profile_name` Prompt: `hostname(config-y1564-profile)#`
JSON Notification Host Config	Config	Sub-mode for configuring JSON notification hosts Command: `json notification host host_name` Prompt: `hostname(config-json-notif-host)#`

It is possible for a user to transition between these modes using certain commands, subject to the user's privilege level and the current session privilege level (see Understanding Privilege Levels, page 1-16).

The initial mode is determined by the privilege level of the user logging in. If the privilege level is zero or one the user is unprivileged and begins in the (Unprivileged) Exec mode. If the privilege level is higher, the session begins in Privileged Exec mode.

A user can raise the Exec mode privilege level to a higher value if an enable password has been configured for that level. This elevation is done with the `enable` level command, where level is a value between 1 and 15. The reverse operation (lowering the privilege level) is achieved with the `disable` command.

Once in Privileged Exec mode, it is possible to enter into the global configuration mode by entering the command `configure terminal`. Exit from global configuration is achieved by typing **end or exit** and then pressing **Enter** or pressing Ctrl-Z**.**

Access to a configuration sub-mode (for example, Ethernet interfaces) goes through global configuration or another sub-mode. Thus, it is possible to change directly from VLAN sub-mode to Ethernet interface sub-mode, for instance.

Thus, each mode and sub-mode implements a scope for commands. Inside each mode, a particular subset of commands is available. To get to other commands, one must generally change mode/sub-mode. This is necessary because there are commands with identical prefixes in different modes. For example, there are commands that begin with 'ip' in Privileged Exec, global configuration, and VLAN Interface Configuration modes.

There are two exceptions to this:

- While in a configuration sub-mode, access to global configuration mode commands is possible as long as there is no ambiguity. Execution of a global configuration command exits the sub-mode.
- Exec mode commands (whether privileged or unprivileged) are accessible from within global configuration or one of the sub-modes by using the `do` command.

The `do` command takes an arbitrary command line from Exec and executes it. In the following example, the user wants to change the IP address on the VLAN 1 interface and uses `do` to verify the current address while in the sub-mode.

Using 'do' While in a Sub-Mode

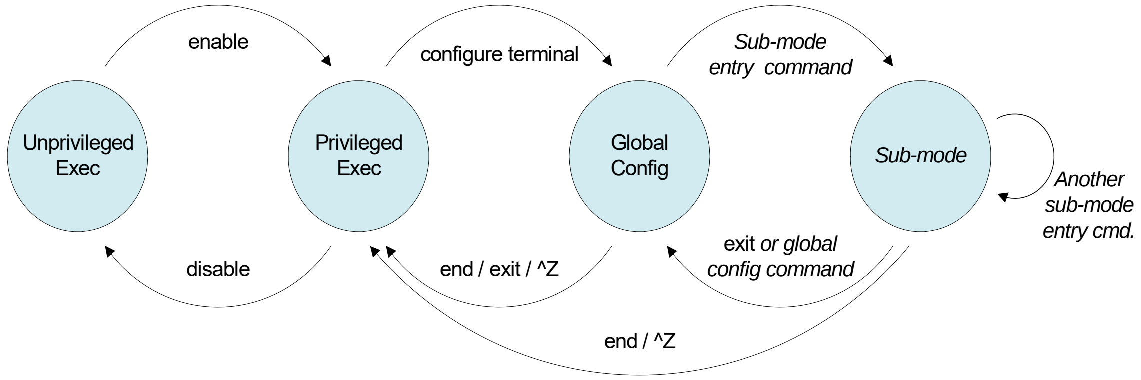
```
my-device# configure terminal
my-device(config)# interface vlan 1
my-device(config-if-vlan)# do show ip interface brief
Vlan Address              Method   Status
---- -------------------- -------- ------
   1 172.16.1.15/24       DHCP     UP
my-device(config-if-vlan)# end
! When in Exec, no 'do' prefix is needed:
my-device# show ip interface brief
```

```
Vlan Address              Method   Status
---- -------------------- -------- ------
   1 172.16.1.15/24       DHCP     UP
```

ICLI Mode Transitions

The following illustration shows the possible transitions between major modes and sub-modes, and some of the relevant commands.

Figure 1 • **ICLI Mode Transitions**



Changing Between ICLI Modes

```
! Initial mode for this example is Unprivileged Exec. Raise level
! (and change mode):
my-device> enable
Password: ***
my-device#

! Note how the prompt changed from '>' to '#' to indicate the privileged
exec mode

! Enter global configuration mode:
my-device# configure terminal

! Now create VLAN 100 and give it a name. This enters the VLAN sub-mode,
as
! indicated by a new prompt:
my-device(config)# vlan 100
my-device(config-vlan)# name MyVlan

! Change directly from VLAN sub-mode into Ethernet interface sub-mode
for
! interface instance 4 on switch 1, and set link speed to 'auto'
my-device(config-vlan)# interface GigabitEthernet 1/4
my-device(config-if)# speed auto

! Then enter a command from the global configuration mode; this leaves
Ethernet
! interface sub-mode
my-device(config-if)# hostname my-device

! Exit global configuration mode and go back to Privileged Exec
my-device(config)# end
```

```
! And use ‘disable’ to go back to Unprivileged Exec:
my-device# disable
my-device>
```

Understanding Privilege Levels

A privilege level is a number in the range of 0 to 15, inclusive, with 0 being the lowest. It is assigned to a user session and used to determine access to ICLI commands. Only commands at the same or lower privilege level can be accessed.

Each user on the device has a default privilege level that is copied to the session’s privilege level at login. It is, however, possible for the user to change the session privilege level by executing the `enable` or `disable` commands. This can be used, for example, as follows:

- The user account is configured with privilege level 0
- Whenever the user needs to perform higher-privileged commands, the user changes session priority level, executes the necessary commands, and then reverts back to the default priority level

Access to higher priority levels must be password protected by using the `enable password or enable secret` global configuration commands. The main difference between the two is whether passwords are displayed in clear text or encrypted form in `running-config`, and consequently, `startup-config`.

Password input can also be in encrypted or clear text form. The latter is used when an operator inputs a new password, as the operator will usually not know the encrypted form of the password.

The admin user is at level 15 by default, the highest possible privilege level.

Configuring Privilege Level Passwords

The following example configures a level 15 password using `enable secret`, inspects the resulting configuration, then removes it again.

```
my-device# configure terminal

! A secret can either be input in clear text or encrypted form; a digit
indicates
! which kind follows on the command line:
my-device(config)# enable secret ?
    0    Specifies an UNENCRYPTED password will follow
    5    Specifies an ENCRYPTED secret will follow

! In this case: Unencrypted. Then follows either the level for which a
password
! is being configured, or, if no level is given, the password for level
15:
my-device(config)# enable secret 0 ?
    <word32>    Password
    level       Set exec level password

! Thus, the following two commands are semantically identical:
my-device(config)# enable secret 0 my-secret
my-device(config)# enable secret 0 level 15 my-secret

! The running configuration can be inspected to see the encrypted form:
my-device(config)# do show running-config | include enable
enable secret 5 level 15 D29441BF847EA2DD5442EA9B1E40D4ED
```

```
! To remove the password use the ‘no’ form (the two are semantically
equivalent for level 15):
my-device(config)# no enable secret
my-device(config)# no enable secret level 15
my-device(config)# do show running-config | include enable
my-device(config)#
```

Understanding Terminal Parameters

Each system login, whether through the serial console or through telnet or ssh, creates a session. The session is initialized with settings that are configurable from the line configuration sub-mode, but most of them can also be changed from Exec mode while the session is active. Such changes are not persistent, however, and are lost when the session is terminated.

The following table lists available settings and modes where each can be configured.

Table 7 • **Setting and Modes**

Setting	Modes	Description
editing	Exec, Line	Enable/disable command line scrolling
exec-banner	Line	Enable/disable display of the Exec banner (configured with ‘banner exec ...’)
exec-timeout	Exec, Line	Inactivity timer; automatically log out after a period of inactivity. A value of zero disables automatic logout
history	Exec, Line	Length of command history buffer
length	Exec, Line	Terminal length in lines, used for pagination. Zero disables pagination
location	Line	A line of text that describes the terminal location (such as “Server room”)
motd-banner	Line	Enable/disable display of Message-Of-The-Day banner (configured with ‘banner motd ...’)
privilege	Line	Assign default privilege level
width	Exec, Line	Terminal width in characters, used for pagination

The following table lists available settings and modes where each can be configured.

The system allows one serial console session and up to 16 network sessions. The console session is called “console 0” whereas each network session is called “vty X” where vty is an abbreviation for Virtual TTY and X is a value between 0 and 15.

The configuration appears near the bottom of *running-config* and looks like this:

```
line console 0
 exec-timeout 0
!
line vty 0
!
line vty 1
!
line vty 2
! [...]
```

It is possible to specify different settings for each vty, but this is generally not recommended since there is no way to associate an incoming ssh or telnet connection with a specific vty.

Changing Terminal Parameters

This example shows how to change some values for the current session, and for all future console sessions.

```
! First inspect current settings for this session:
my-device# show terminal
Line is con 0.
    * You are at this line now.
    Alive from Console.
    Default privileged level is 2.
    Command line editing is enabled
    Display EXEC banner is enabled.
    Display Day banner is enabled.
    Terminal width is 80.
             length is 24.
             history size is 32.
             exec-timeout is 10 min 0 second.

    Current session privilege is 15.
    Elapsed time is 0 day 0 hour 15 min 42 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.

! Then set terminal length to zero to disable pagination, and
exec-timeout to
! zero to disable automatic logout:
my-device# terminal length 0
my-device# terminal exec-timeout 0
my-device# show terminal
Line is con 0.
    * You are at this line now.
    Alive from Console.
    Default privileged level is 2.
    Command line editing is enabled
    Display EXEC banner is enabled.
    Display Day banner is enabled.
    Terminal width is 80.
             length is 0.
             history size is 32.
             exec-timeout is 0 min 0 second.

    Current session privilege is 15.
    Elapsed time is 0 day 0 hour 16 min 31 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.

! Then we do the same, but for all future console sessions. Note how the
commands
! have no ‘terminal’ prefix (‘terminal length’ vs. ‘length’):
my-device# configure terminal
my-device(config)# line console 0
my-device(config-line)# exec-timeout 0
my-device(config-line)# length 0
my-device(config-line)# end
```

```
! Finally save the configuration to startup-config to make it
persistent:
my-device# copy running-config startup-config
Building configuration...
% Saving 1287 bytes to flash:startup-config
my-device#
```

Using Banners

The system provides three different banners (text that is output as messages to the user):

- The Message Of The Day banner (MOTD), displayed upon connection to the system or when a console login attempt has timed out
- The Login banner, displayed before the first “Username:” login prompt
- The Exec banner, displayed upon successful login

All of these banners are configured in a similar manner, using the `banner` command:

banner [motd] *banner*

banner exec *banner*

banner login *banner*

The banner text can be either a single line or multiple lines. The first character of the text defines a delimiter character; the actual text of the banner then follows and ends at the first appearance of the delimiter character. The delimiters are not included in the actual text.

Configuring Banners

```
! First configure the MOTD banner, which in this case is multi-line. ‘*’
is
! used as delimiter character, but any printable character that isn’t
used in
! the message is usable:
my-device# configure terminal
my-device(config)# banner motd *This is the Message Of The Day Banner.
Enter TEXT message.  End with the character '*'.
It spans multiple lines.
And one more. But now it ends.*

! Then the Login and Exec banners. Both are single-line. Note how
different
! delimiters are used in each banner:
my-device(config)# banner login XThis is my-device.X
my-device(config)# banner exec “WARNING: Production system. Be
careful.”
my-device(config)# end

! Inspect configuration:
my-device# show running-config
Building configuration...
banner motd "This is the Message Of The Day Banner.
It spans multiple lines.
And one more. But now it ends."
banner exec "WARNING: Production system. Be careful."
banner login "This is my-device."
hostname my-device
! [...]
end
```

```
! Test it: Log out, then log in again:
my-device# exit

This is the Message Of The Day Banner.
It spans multiple lines.
And one more. But now it ends.

Press ENTER to get started<ENTER>

This is my-device.

Username: admin
Password:

WARNING: Production system. Be careful.
my-device#

! Finally save the configuration to startup-config to make it
persistent:
my-device# copy running-config startup-config
Building configuration...
% Saving 1461 bytes to flash:startup-config
my-device#
```

Configuring the System

Changes to system configuration can only be made from the global configuration mode and its sub-modes, except when working with configuration files or reloading defaults. This is done in Privileged Exec mode. The following steps outline the sequence.

1. Raise privilege level to 15.
2. Enter global configuration mode.
3. Input appropriate configuration commands. Optionally, enter sub-modes and input appropriate commands there.
4. Exit global configuration mode.
5. Verify configuration.
6. Save configuration to flash.

Configuration Example

In this example, the hostname and VLAN 1 IP address is configured, verified, and saved. This example assumes the session is initially unprivileged.

1. Raise privilege level:

```
> enable
Password: ***
```

2. Enter global configuration mode:

```
# configure terminal
```

3. Input configuration commands. The IP address is set from within the

```
! VLAN interface submode:
(config)# hostname my-device
my-device(config)# interface vlan 1
my-device(config-if-vlan)# ip address dhcp fallback 172.16.1.2
255.255.0.0
```

```
my-device(config-if-vlan)# exit
```

4. Leave global configuration mode and go back to Privileged Exec:

```
my-device(config)# end
```

5. Inspect and verify the configuration (some output omitted for brevity):

```
my-device# show running-config
Building configuration...
hostname my-device
username admin privilege 15 password encrypted
3ad61dc090116a16a7cc9861485e60e6407c5a328015b1985b585ab353c37a4441e034
172401528229795a5c9529dfbc04c86e01
!
vlan 1
 name default
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
...
interface vlan 1
 ip address dhcp fallback 172.16.1.2 255.255.0.0
!
...
end
! More verification: Display IP interfaces and assigned IP address and
status:
my-device# show ip interface brief
Vlan Address              Method   Status
---- -------------------- -------- ------
   1 172.16.1.15/24       DHCP     UP
! An address was obtained from DHCP, so the fallback wasn’t used
! Try to inspect hostname:
my-device# show hostname
                ^
% Invalid word detected at '^' marker.
! No such command exists, but it is possible to extract a single line
from
! running-config by using a filter:
my-device# show running-config | include hostname
hostname my-device
```

6. Save configuration to flash:

```
my-device# copy running-config startup-config
Building configuration...
% Saving 1272 bytes to flash:startup-config
```

Resetting or Removing Configuration with "no"

It is possible to remove specific configuration items or reset them to their default values. In general, almost each configuration command has a corresponding **no** form. The ‘no’ form is syntactically similar (but not necessarily identical) to the configuration command, but either resets the parameters to defaults for the configurable item being addressed or removes the item altogether.

In many cases, ‘’no’’ can be read as no(t) different from default settings.

Using "no" Forms

The following list shows the tasks accomplished:

- Configure the VLAN 1 interface IP address to use DHCP
- Configure the DNS name server to be taken from DHCP
- Inspect the configuration
- Remove the DNS name server
- Remove the IP address on the VLAN 1 interface

Both ‘’no” operations can be viewed as reset-to-default, with the defaults being no DNS name server and no IP address.

```
my-device# configure terminal
my-device(config)# interface vlan 1
my-device(config-if-vlan)# ip address dhcp
my-device(config-if-vlan)# exit
my-device(config)# ip name-server dhcp
my-device(config)# end

my-device# show ip interface brief
Vlan Address             Method   Status
---- ------------------- -------- ------
   1 172.16.1.15/24      DHCP     UP
my-device# show ip name-server
Current DNS server is 172.16.1.1 set by DHCP.
my-device# configure terminal
my-device(config)# no ip name-server
my-device(config)# interface vlan 1
my-device(config-if-vlan)# no ip address\
my-device(config-if-vlan)# end
my-device# show ip name-server
Current DNS server is not set.
my-device# show ip interface brief
Vlan Address             Method   Status
---- ------------------- -------- ------
my-device#
```

Note: The syntax of the configuration commands and their ‘no’ forms are different; the ‘no’ forms usually do not take as many parameters.

This is usually convenient but may give surprising results in certain cases. For example, an OAM MEP instance can configure Continuity Check using ‘`mep` *num* `cc` *priority* ...’ and reset it with ‘`no mep` *num* `cc`’. However, because MEPs are removed using the command ‘`no mep` *num*’, it is possible to unintentionally remove an existing MEP by entering ‘`no mep 10 ccc`’ – the extra ‘c’ means that the last word isn’t recognized as ‘cc’, leading to a match of the MEP removal command instead of the desired reset-CC command.

Managing Users

The following describes local user management on the device. RADIUS and TACACS+ user management is beyond the scope of this document.

It is possible to create several user accounts on a system. Each user account has a set of configurable attributes:

- User name
- Password
- Privilege level

All attributes are configured with the same command, `username.`

```
username username privilege level password { unencrypted | encrypted }
password
username username privilege level password none
no username username
```

The command `password none` is used when no password is desired. The security implications of using this should be considered carefully. Likewise, `no username` deletes the given user account.

Adding, Modifying, and Deleting Users

The following example adds two user accounts at different privilege levels, inspects configuration, and deletes one account again using ‘no username’.

```
! Display current set of local user accounts:
my-device# show running-config | include username
username admin privilege 15 password encrypted
3ad61dc090116a16a7cc9861485e60e6407c5a328015b1985b585ab353c37a4441e034
172401528229795a5c9529dfbc04c86e01

! Add two accounts, ‘operator’ and ‘monitor’. The passwords are supplied
in
! unencrypted form:
my-device# configure terminal
my-device(config)# username operator privilege 10 password unencrypted
a-secret
my-device(config)# username monitor privilege 1 password unencrypted
new-secret

! Verify that the configuration is correct. Note that passwords are
displayed
! in encrypted form:
my-device(config)# do show running-config | include username
username admin privilege 15 password encrypted
3ad61dc090116a16a7cc9861485e60e6407c5a328015b1985b585ab353c37a4441e034
172401528229795a5c9529dfbc04c86e01
username operator privilege 10 password encrypted
015b1985b585ab353c37a4441e034172401528229795a5c9529dfbc04c86e012138abc
d88dda222affea861485e60e6407c5a328
username monitor privilege 1 password encrypted
7cc9861485e60e6407c56a16a7cc9861485e60e6407c5a328441e03417240152822979
5a5c95229795a5c9529dfbc04c86e01abc

! Delete the ‘operator’ user and verify it is removed from the
configuration:
my-device(config)# no username operator
my-device(config)# do show running-config | include username
username admin privilege 15 password encrypted
ad61dc090116a16a7cc9861485e60e6407c5a328015b1985b585ab353c37a4441e0341
72401528229795a5c9529dfbc04c86e01
username monitor privilege 1 password encrypted
7cc9861485e60e6407c56a16a7cc9861485e60e6407c5a328441e03417240152822979
5a5c95229795a5c9529dfbc04c86e01abc
```

Using Show Commands

The family of show commands is the cornerstone of ICLI-based system monitoring. Most features implement one or more show commands that will display a relevant mix of status and configuration.

Note: The exact set of available commands, parameters, and output format depends on the system configuration and software version, so some of the following commands and examples may not be applicable to all systems.

The show commands exist only in the two Exec modes and are subject to session privilege level enforcement. Therefore, listing the largest possible set of show commands requires the session to be at level 15.

Listing All show Commands

The following example raises the session privilege level to 15. In this example, an enable secret has been specified, so password entry is required to proceed. Then the user inputs show and uses the context-sensitive help feature to list the possible show commands, in this case for a Carrier Ethernet system.

```
my-device> enable
Password: ***
my-device# show ?
    aaa                Login methods
    access             Access management
    access-list        Access list
    aggregation        Aggregation port configuration
    clock              Configure time-of-day clock
   dot1x            IEEE Standard for port-based Network Access Control
    eps                Ethernet Protection Switching
    erps               Ethernet Ring Protection Switching
    evc                Ethernet Virtual Connections
    green-ethernet     Green ethernet (Power reduction)
    history            Display the session command history
    interface          Interface status and configuration
    ip                 Internet Protocol
    ipmc               IPv4/IPv6 multicast configuration
    ipv6               IPv6 configuration commands
    lacp               LACP configuration/status
    line               TTY line information
    link-oam           Link OAM configuration
    lldp               Display LLDP neighbors information.
    logging            Syslog
    loop-protect       Loop protection configuration
    mac                Mac Address Table information
    mep                Maintenance Entity Point
    mvr                Multicast VLAN Registration configuration
    network-clock      Show selector state.
    ntp                Configure NTP
    perf-mon           Performance Monitor
    platform           Platform specific information
    port-security      Port security
    privilege          Display command privilege
    ptp                Precision time Protocol (1588)
    pvlan              PVLAN configuration
    qos                Quality of Service
    radius-server      RADIUS configuration
    rfc2544            RFC2544 perfomance tests
    rmon               RMON statistics
    running-config     Show running system information
    sflow              Statistics flow.
    snmp               Display SNMP configurations
    spanning-tree      STP Bridge
    switchport         Display switching mode characteristics
    tacacs-server      TACACS+ configuration
    terminal           Display terminal configuration parameters
    thermal-protect    Display thermal protection status.
    upnp               Display UPnP configurations
    users              Display information about terminal lines
    version            System hardware and software status
    vlan               VLAN status
    voice              Voice appliance attributes
    web                Web
```

Using Context-sensitive Help for Discovery

The context-sensitive help feature for syntax display is also useful for determining the exact command to execute. In the following example, the user discovers the proper command `show ip statistics system` through exploration:

```
my-device# show ip ?
    arp            Address Resolution Protocol
    dhcp           Dynamic Host Configuration Protocol
    http           Hypertext Transfer Protocol
    igmp           Internet Group Management Protocol
    interface      IP interface status and configuration
    name-server    Domain Name System
    route          Display the current ip routing table
    source         source command
    ssh            Secure Shell
    statistics     Traffic statistics
    verify         verify command

my-device# show ip statistics ?
    |            Output modifiers
    icmp         IPv4 ICMP traffic
    icmp-msg     IPv4 ICMP traffic for designated message type
    interface    Select an interface to configure
    system       IPv4 system traffic
    <cr>

! A repeated press of '?' displays the syntax:
my-device# show ip statistics ?
show ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ]
[ icmp-msg <type> ]

my-device# show ip statistics system

IPv4 statistics:

  Rcvd:  2768 total in 181458 bytes
         1727 local destination, 0 forwarding
         0 header error, 0 address error, 0 unknown protocol
         0 no route, 0 truncated, 0 discarded
  Sent:  2553 total in 180047 bytes
         1512 generated, 0 forwarded
         0 no route, 0 discarded
  Frags: 0 reassemble (0 reassembled, 0 couldn't reassemble)
         0 fragment (0 fragmented, 0 couldn't fragment)
         0 fragment created
  Mcast: 0 received in 0 byte
         0 sent in 0 byte
  Bcast: 0 received, 0 sent
```

show running-config

The virtual file *running-config* consists of a list of commands that, taken together, result in the currently running system configuration.

This list of commands is usually not 100% identical to the list of commands a user has input to configure the device. That is because *running-config* is a textual representation of the system configuration that is stored in binary form in the RAM memory of the device.

Because the effective device configuration is huge, *running-config* in the majority of cases only lists the delta between default settings and current settings. This significantly reduces the amount of output and greatly improves readability of the configuration, but it does require the reader to know what the default settings are.

With **show running-config all-defaults**, it is possible to include values that are at default.

Default vs. Non-default vs. All Defaults

In this example, if the speed and duplex settings of an Ethernet interface are at default values (auto-negotiation), then nothing will be output. If the user then changes the speed to be fixed at 1 Gbps, then that value is now non-default and will be output. Duplex is also output because it is forced to ‘full’ when the speed is fixed at 1 Gbps.

```
! Display current configuration for an interface. All settings are at
default:
my-device# show running-config interface GigabitEthernet 1/4
Building configuration...
interface GigabitEthernet 1/4
!
end

! Now set the speed to 1Gbps and display the configuration again:
my-device# configure terminal
my-device(config)# interface GigabitEthernet 1/4
my-device(config-if)# speed 1000
my-device(config-if)# end

my-device# show running-config interface GigabitEthernet 1/4
Building configuration...
interface GigabitEthernet 1/4
 speed 1000
 duplex full
!
end

! Include all default settings for that interface:
```

```
my-device# show running-config interface GigabitEthernet 1/4
all-defaults
Building configuration...
interface GigabitEthernet 1/4
 switchport voice vlan mode disable
 no switchport voice vlan security
 switchport voice vlan discovery-protocol oui
 loop-protect
 no loop-protect action
 loop-protect tx-mode
 switchport access vlan 1
 switchport trunk native vlan 1
 switchport hybrid native vlan 1
! ... much output omitted for brevity ...
```

The output of **show running-config** can be restricted to a specific interface. There are several such filters, described below.

show running-config [all-defaults]

This displays the entire currently-running system configuration.

show running-config feature feature_name [all-defaults]

Only output the commands relevant to a particular feature. The feature list depends on system configuration and software version. For example:

```
my-device# show running-config feature ?
    CWORD   Valid words are 'GVRP' 'access' 'access-list' 'aggregation'
             'arp-inspection' 'auth' 'clock' 'dhcp' 'dhcp-snooping'
             'dhcp_server' 'dns' 'dot1x' 'eps' 'erps' 'evc'
'green-ethernet'
             'http' 'icli' 'ip-igmp-snooping' 'ip-igmp-snooping-port'
           'ip-igmp-snooping-vlan' 'ipmc-profile' 'ipmc-profile-range'
'ipv4'
             'ipv6' 'ipv6-mld-snooping' 'ipv6-mld-snooping-port'
            'ipv6-mld-snooping-vlan' 'lacp' 'link-oam' 'lldp' 'logging'
           'loop-protect' 'mac' 'mep' 'monitor' 'mstp' 'mvr' 'mvr-port'
          'network-clock' 'ntp' 'perf-mon' 'phy' 'port' 'port-security'
            'ptp' 'pvlan' 'qos' 'rfc2544' 'rmon' 'snmp' 'source-guard'
'ssh'
             'thermal-protect' 'upnp' 'user' 'vlan' 'voice-vlan'
             'web-privilege-group-level'

my-device# show running-config feature dns
Building configuration...
!
vlan 1
!
!
!

ip dns proxy
!
interface GigabitEthernet 1/1
...
```

The structure of *running-config* is maintained in the output. Sub-modes such as VLANs and Ethernet interfaces are listed, but may be empty if the requested feature is irrelevant for the particular sub-mode.

show running-config interface list [all-defaults]

By using this filter, the user can review a specific list of Ethernet interfaces. This may contain wildcards, for example:

```
my-device# show running-config interface GigabitEthernet *
Building configuration...
interface GigabitEthernet 1/1
 speed 1000
 duplex full
!
interface GigabitEthernet 1/2
!
end
```

In this example, there is only one VLAN on the system.

show running-config interface vlan list [all-defaults]

It is also possible to filter the list of VLAN interface, for example:

```
my-device# show running-config interface vlan 1-10
Building configuration...
interface vlan 1
 ip address dhcp fallback 172.16.1.2 255.255.0.0
!
end
```

In this example, there is only one VLAN interface on the system.

show running-config line { console | vty } list [all-defaults]

This command can be used for the console or list of virtual terminal devices (vty). On current designs, there is a single console device, 0. For example:

```
my-device# show running-config line console 0
Building configuration...
line console 0
 exec-timeout 0 0
!
end
```

Working with Configuration Files

There are four kinds of configuration files:

- running-config – a virtual file containing the currently running system configuration.
- startup-config – contains the boot-time configuration. When configuration is changed, it must be copied to *startup-config* in order to be applied at the next boot.
- default-config – a read-only file used when configuration is restored to defaults. This file is also used if *startup-config* is missing. It contains product-specific customizations to the default settings of the device.

- User-defined – configuration files created by the user (up to 31). These are typically used for backups or variants of *startup-config.*

All of these except *running-config* are stored in the flash file system. The available operations are:

copy *source destination*

where source and destination can be one of:

- `running-config`
- `startup-config (or flash:startup-config)`
- `flash:filename`
- `tftp://server[:port]/path-to-file`

```
dir
```

List the contents of the flash file system.

```
more flash: filename
```

Outputs the contents of the file to the terminal.

```
delete flash: filename
```

Erases the specific file.

Reverting to Default Configuration

It is possible to reset the system to a default configuration in two ways:

- Deleting *startup-config* and rebooting
- Instructing the software to discard the current configuration and reset to defaults without rebooting

Deleting *startup-config* doesn't change *running-config* until the system is rebooted, at which time the defaults are loaded.

Conversely, discarding the current configuration does indeed affect *running-config* but does not touch *startup-config*. An explicit `copy running-config startup-config` is necessary to make the change persistent.

Rebooting and resetting the default configuration is accomplished with the `reload` command:

```
reload cold [ sid switch_id ]
reload defaults [ keep-ip ]
```

The reload cold version reboots the system. If the system is stacking, a specific switch can be rebooted as well by supplying its switch ID.

The second method loads configuration defaults. If the `keep-ip` keyword is given, then the system attempts to keep the most relevant parts of the VLAN 1 IP setup in order to maintain management connectivity (the IP address setup and the active default route).

There is no guarantee, however, that the above is sufficient for reverting to default configuration: it depends on the actual network properties and the system's total IP configuration. In some cases, it may be preferable to explicitly un-configure the system using 'no' commands, or prepare a suitable configuration and download it to the system's *startup-config* and reboot.

Working with Configuration Files

The following example assumes a file system that contains an additional file called *backup*, previously created with a `copy` command.

```
! List files in flash:
my-device# dir
Directory of flash:
    r- 1970-01-01 00:00:00      648 default-config
    rw 1970-01-06 03:57:33     1313 startup-config
    rw 1970-01-01 19:54:01     1237 backup
3 files, 3198 bytes total.

! Display the contents of the file ‘backup’ (output is abbreviated):
my-device# more flash:backup
hostname my-device
...
end
! Use file ‘backup’ for the next boot by overwriting startup-config:
my-device# copy flash:backup startup-config
% Saving 1237 bytes to flash:startup-config

! Verify that the sizes are identical:
my-device# dir
Directory of flash:
    r- 1970-01-01 00:00:00      648 default-config
    rw 1970-01-06 05:30:41     1237 startup-config
    rw 1970-01-01 19:54:01     1237 backup
3 files, 3122 bytes total.

! Regret and delete startup-config. Note how ‘flash:’ is required:
my-device# delete flash:startup-config
my-device# dir
Directory of flash:
    r- 1970-01-01 00:00:00      648 default-config
    rw 1970-01-01 19:54:01     1237 backup
2 files, 1885 bytes total.

! Use the currently running config for next boot:
my-device# copy running-config startup-config
Building configuration...
% Saving 1271 bytes to flash:startup-config
```

Using Reload Commands

```
! Reload defaults, but try to keep VLAN 1 configuration. First list
current IP
! settings:
my-device# show ip interface brief
Vlan Address              Method   Status
---- -------------------- -------- ------
   1 172.16.1.17/24       DHCP     UP

my-device# reload defaults keep-ip
% Reloading defaults, attempting to keep VLAN 1 IP address. Please stand
by.
# show ip interface brief
Vlan Address              Method   Status
---- -------------------- -------- ------
   1 172.16.1.17/24       DHCP     UP

! Contents of flash: are unchanged:
```

```
my-device# dir
Directory of flash:
    r- 1970-01-01 00:00:00      648 default-config
    rw 1970-01-06 05:33:18     1237 startup-config
    rw 1970-01-01 19:54:01     1237 backup
3 files, 3122 bytes total.

! Reload again, but don't try to keep VLAN 1 settings:
# reload defaults
% Reloading defaults. Please stand by.
! Verify that the default IP settings have been restored:
# show ip interface brief
Vlan Address              Method   Status
---- -------------------- -------- ------
   1 192.0.2.1/24         Manual   UP

! Reboot the system
# reload cold
% Cold reload in progress, please stand by.
! ... bootup output omitted ...
```

Working with Software Images

The system can store up to two software images in flash. The image selected for bootup is termed the Active image, while the other is termed the Alternate image.

It is possible to swap the Active and the Alternative image, and it is possible to upgrade to a new Active image. A swap simply switches the Active and Alternate designation on each image and reboots the system.

A firmware upgrade performs these steps:

- Download new firmware using TFTP/HTTP/HTTPS/FTP and verify suitability for the system
- Overwrite the current Alternate image with the newly downloaded image
- Swap Active and Alternate and reboot

The result is that the old Active build becomes the Alternate, and the newly downloaded image Active.

The relevant commands are:

```
show version

firmware swap

firmware upgrade protocol tftp://server[:port]/path_to_file
```

`show version` lists various details about the system, including the images in flash.

Configure IP Static Routes

An IP address identifies a device on an IP network. The IP version 4 (IPv4) address is 32 bits long. An IPv4 address can only be assigned through a VLAN interface. The address can be set manually (called a static IP) or automatically by using the DHCP protocol. For more information, see Configure the DHCP Client. The switch application software implements software to handle static IPv4 routing.

Traditional Network

Routing involves both a TCP/IP host and an IP router. The following illustration shows the configuration for a traditional network with two IP networks and a router. Each IP network needs to have an IP address assigned and a gateway where packets can be forwarded to.

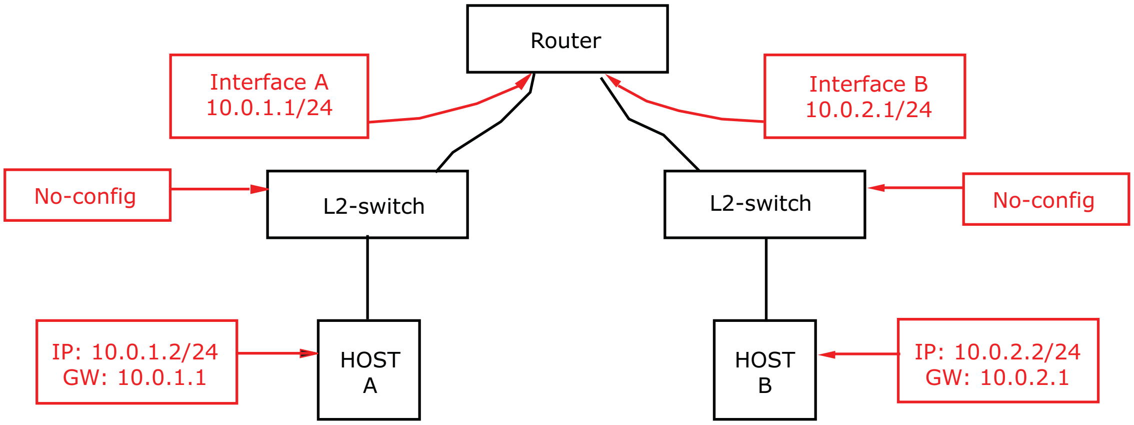


***Figure 1* • IP Routing using a Router and Switches**

Using a VLAN-Aware Switch

The following illustration shows the same network configured to use a VLAN-aware switch. Using VLANs is a method of separating flows within the same switch.

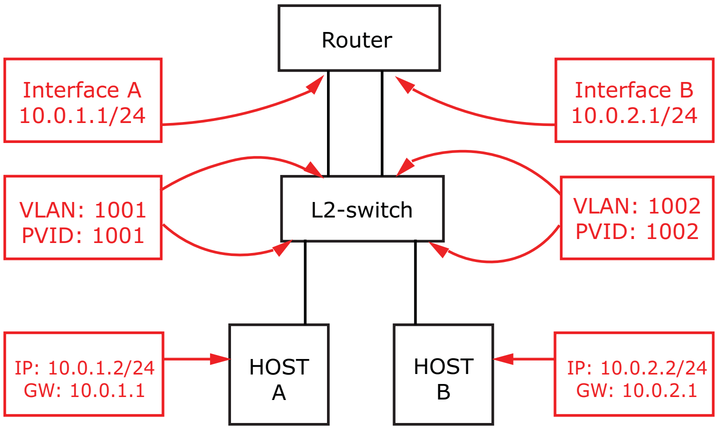


Figure 2 • **IP Routing using a Router and VLAN-Aware Switch**

Using a Layer 3 Switch

The following illustration shows the same network configured to use an L3 switch.

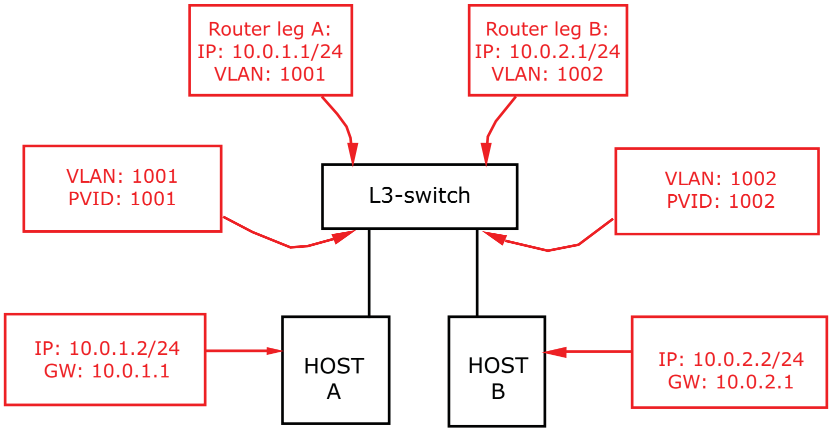


Figure 3 • **IP Routing using a Router and L3 Switch**

IP routing is fundamentally a destination-driven process. All frames that enter the router are inspected to determine the destination IP address. Based on that address the router looks up the routing table to determine where to send the frame.

Configuration using ICLI

The following steps implement the configurations using the command line interface.

1. Step 1: Create VLAN 1001 and 1002 to separate the two IP networks

```
Switch# configure terminal
```

```
Switch(config)# vlan 1001
Switch(config-vlan)# vlan 1002
Switch(config-vlan)# exit
```

2. Step 2: Define the port VLAN for each port by using the `switchport access vlan` command to specifiy the VLAN for each interface. Untagged frames are then classified to this VLAN.

```
Switch(config)# interface GigabitEthernet 1/1
Switch(config-if)# switchport access vlan 1001
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet 1/2
Switch(config-if)# switchport access vlan 1002
Switch(config-if)# exit
```

3. Step 3: Configure router leg A and B by using the `ip address` command to set primary IP address for the interfaces.

```
Switch(config)# interface vlan 1001
Switch(config-if-vlan)# ip address 10.0.1.1 255.255.255.0
Switch(config-if-vlan)# exit
Switch(config)# interface vlan 1002
Switch(config-if-vlan)# ip address 10.0.2.1 255.255.255.0
Switch(config-if-vlan)# end
```

Connecting Two L3 Switches

The following illustration shows how two L3 switches can be interconnected.

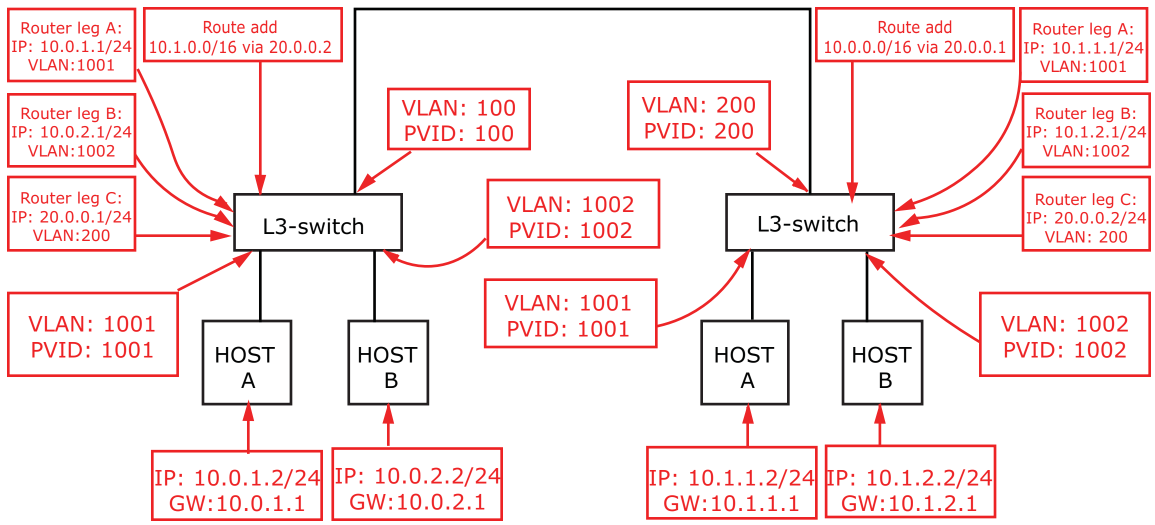


Figure 4 **• IPv4 Static Route**

The following steps implement the configurations using the command line interface.

1. Step 1: Create VLAN 100, 1001, and 1002. Set up port VLAN for each port on the left switch.

```
Switch-left# configure terminal
Switch-left(config)# vlan 100
Switch-left(config-vlan)# vlan 1001
Switch-left(config-vlan)# vlan 1002
Switch-left(config-vlan)# exit
Switch-left(config)# interface GigabitEthernet 1/1
Switch-left(config-if)# switchport access vlan 1001
Switch-left(config-if)# exit
```

```
Switch-left(config)# interface GigabitEthernet 1/2
Switch-left(config-if)# switchport access vlan 1002
Switch-left(config-if)# exit
Switch-left(config)# interface GigabitEthernet 1/6
Switch-left(config-if)# switchport access vlan 100
Switch-left(config-if)# exit
```

2. Step 2: Configure router leg A, B, and C to set IP address for each interface on the left switch.

```
Switch-left(config)# interface vlan 1001
Switch-left(config-if-vlan)# ip address 10.0.1.1 255.255.255.0
Switch-left(config-if-vlan)# exit
Switch-left(config)# interface vlan 1002
Switch-left(config-if-vlan)# ip address 10.0.2.1 255.255.255.0
Switch-left(config-if-vlan)# exit
Switch-left(config)# interface vlan 100
Switch-left(config-if-vlan)# ip address 20.0.0.1 255.255.255.0
Switch-left(config-if-vlan)# exit
```

3. Step 3: Configure IP route on the left switch by using the `ip route` command to add a static route entry with next-hop set to 20.0.0.2.

```
Switch-left(config)# ip route 10.1.0.0 255.255.0.0 20.0.0.2
Switch-left(config)# end
```

4. Step 4: Show the static route's for the left switch.

```
Switch-left# show ip route
0.0.0.0/0 via 10.10.132.1 <UP GATEWAY HW_RT>
10.0.1.0/24 via interface index 200001001 <UP HW_RT>
10.0.2.0/24 via interface index 200001002 <UP HW_RT>
10.1.0.0/16 via 20.0.0.2 <UP GATEWAY HW_RT>
10.10.132.0/23 via interface index 200000001 <UP HW_RT>
127.0.0.1/32 via 127.0.0.1 <UP HOST>
Switch-left#
```

5. Step 5: Create VLAN 200, 1001, and 1002. Set up port VLAN for each port on the right switch.

```
Switch-right# configure terminal
Switch-right(config)# vlan 200
Switch-right(config-vlan)# vlan 1001
Switch-right(config-vlan)# vlan 1002
Switch-right(config-vlan)# exit
Switch-right(config)# interface GigabitEthernet 1/1
Switch-right(config-if)# switchport access vlan 1001
Switch-right(config-if)# exit
Switch-right(config)# interface GigabitEthernet 1/2
Switch-right(config-if)# switchport access vlan 1002
Switch-right(config-if)# exit
Switch-right(config)# interface GigabitEthernet 1/6
Switch-right(config-if)# switchport access vlan 200
Switch-right(config-if)# exit
```

6. Step 6: Configure router leg A, B, and C to set IP address for each interface on the right switch.

```
Switch-right(config)# interface vlan 1001
Switch-right(config-if-vlan)# ip address 10.1.1.1 255.255.255.0
Switch-right(config-if-vlan)# exit
Switch-right(config)# interface vlan 1002
Switch-right(config-if-vlan)# ip address 10.1.2.1 255.255.255.0
Switch-right(config-if-vlan)# exit
Switch-right(config)# interface vlan 200
Switch-right(config-if-vlan)# ip address 20.0.0.2 255.255.255.0
Switch-right(config-if-vlan)# exit
```

7. Step 7: Configure IP route on the right switch by using the `ip route` command to add a static route entry with next-hop set to 20.0.0.1.

```
Switch-right(config)# ip route 10.0.0.0 255.255.0.0 20.0.0.1
Switch-right(config)# end
```

CHAPTER 3

Layer 2 Protocol Configuration

This document describes how to configure Cisco ME1200 Switch Engines to perform Layer 2 functions such as Link Aggregation (LAG), Link Aggregation Control Protocol (LACP), Virtual LANs (VLANs), Mirroring, Generic VLAN Registration Protocol (GVRP), and Multiple Spanning Tree Protocol (MSTP). Configuration examples are provided both for the command line interface (CLI) and the Web GUI.

Aggregation

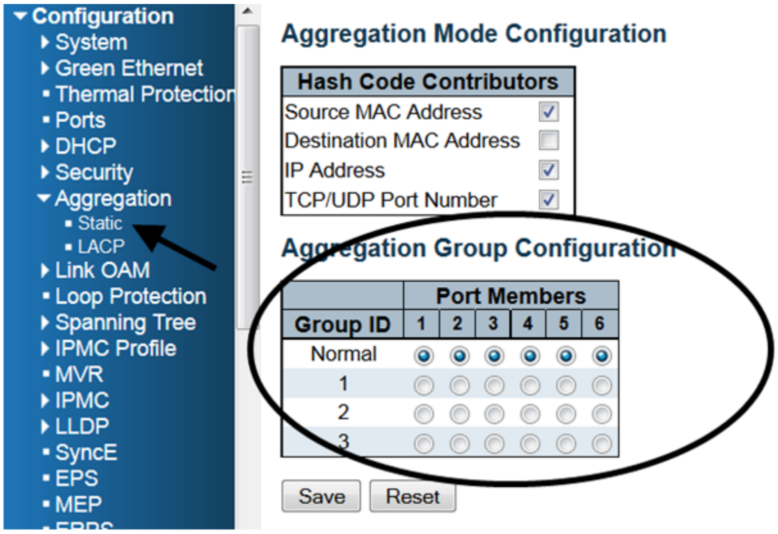
Aggregation enables the use of multiple ports in parallel to increase the link speed beyond the limits of a single port, and to increase the redundancy for higher availability. If the system has 6 ports, the maximum aggregation group is 3 (6 divided by 2).

Adding a Port to an Aggregation Group

CLI Example: Add the first Gigabit port into group 1

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# aggregation ?
    group    Create an aggregation group
(config-if)# aggregation group
<uint>
```

```
(config-if)# aggregation group 1
```



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	○	○	○	○	○	○

Figure 1 **• Aggregation Group Configuration**

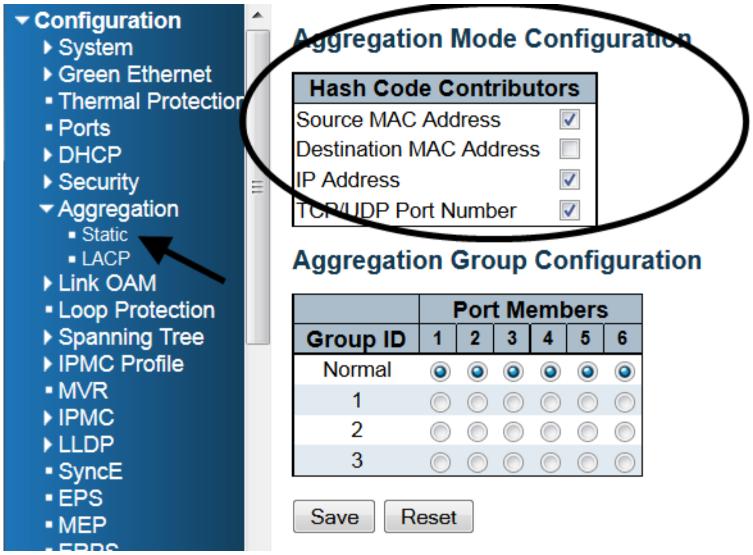
Configuring the Aggregation Mode

The aggregation feature uses the following keys to calculate the destination port for the frame. The default method is the source MAC address, IP address, and TCP/UDP port number. The destination MAC address is not used in the default case.

CLI Example: Change aggregation mode to dmac, ip, port, and smac

```
# configure terminal
(config)# aggregation mode ?
    dmac    Destination MAC affects the distribution
    ip      IP address affects the distribution
    port    IP port affects the distribution
    smac    Source MAC affects the distribution
    <cr>
(config)# aggregation mode dmac ip port smac
(config)# do show aggregation mode
Aggregation Mode:

SMAC  : Enabled
DMAC  : Enabled
IP    : Enabled
```

```
Port  : Enabled
```



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	○	○	○	○	○	○

Figure 2 • **Aggregation Mode Configuration**

The current aggregation mode can be viewed using the **show aggregation mode** command.

```
# show aggregation mode
Aggregation Mode:

SMAC  : Enabled
DMAC  : Disabled
IP    : Enabled
Port  : Enabled
```

LACP

Link Aggregation Control Protocol (LACP) is an IEEE 802.3ad standard protocol that allows bundling several physical ports together to form a single logical port.

Enabling LACP

When LACP is enabled on a port, with the **lacp** command, it will form an aggregation when 2 or more ports are connected to the same partner. The default value is disabled.

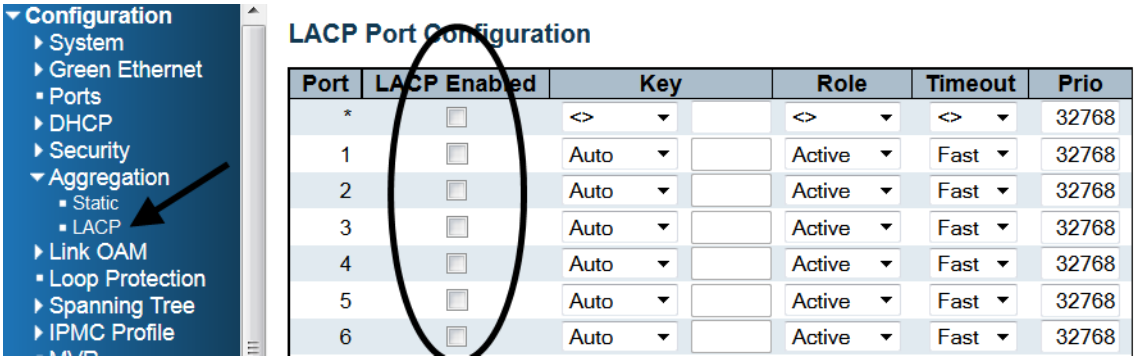
CLI Example: Enable LACP on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# lacp
```

CLI Example: Disable LACP on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
```

```
(config-if)# no lacp
```



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	☐	Auto		Active	Fast	32768

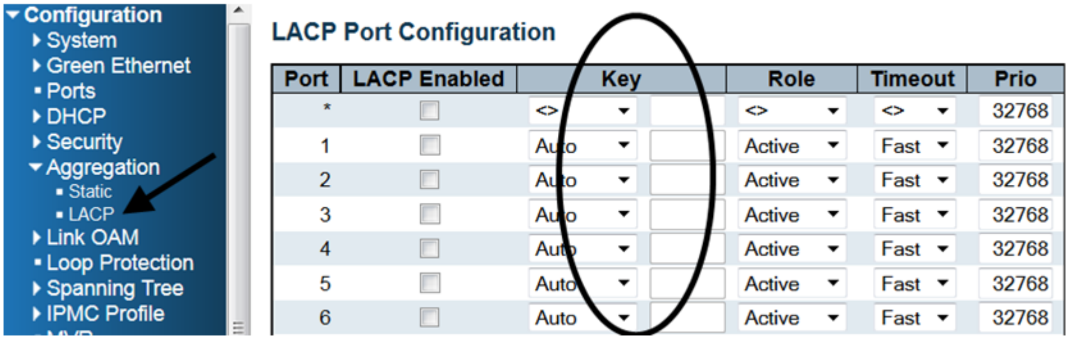
Figure 3 • **LACP Enabled Configuration**

Configuring the Key

The port's LACP key ranges from 1-65535. The Auto setting sets the key according to the physical link speed, 10 Mb = 1, 100 Mb = 2, 1 Gb = 3. With a specific setting a user-defined value can be entered. Ports with the same key can participate in the same aggregation group while ports with different keys cannot. The default value is auto.

CLI Example: Set LACP key to 3 on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# lacp key ?
    <1-65535>    Key value
    auto         Choose a key based on port speed
(config-if)# lacp key 3
```



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	☐	Auto		Active	Fast	32768

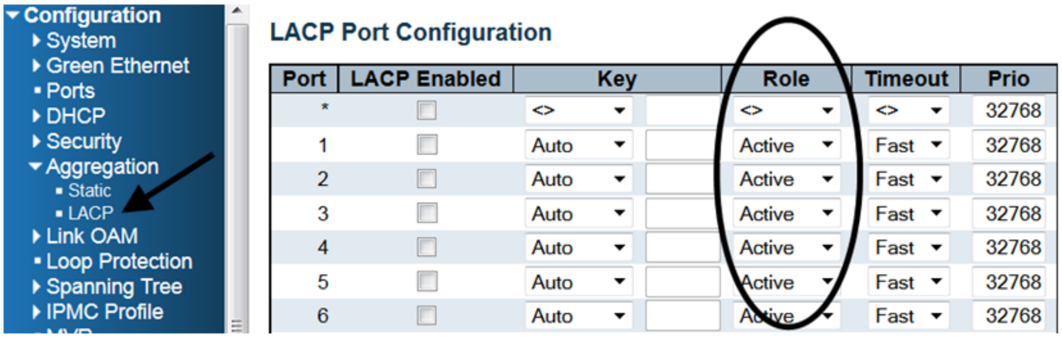
Figure 4 • **LACP Key Configuration**

Configuring the Role

LACP role shows the activity status. An Active role transmits LACP packets each second, while Passive waits for an LACP packet from a partner, also known as the "speak if spoken to" role. The default value is active.

CLI Example: Set LACP Role to Passive on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# lacp role ?
    active     Transmit LACP BPDUs continously
    passive    Wait for neighbour LACP BPDUs before transmitting
(config-if)# lacp role passive
```



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	□	Auto ▾		Active ▾	Fast ▾	32768

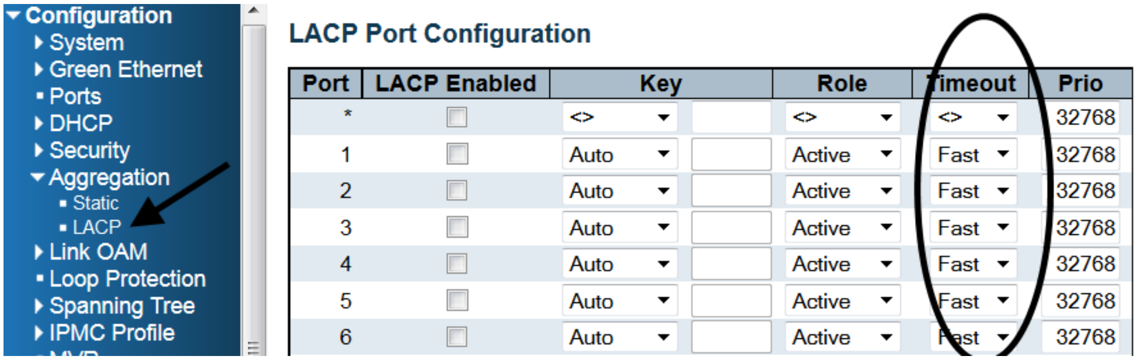
Figure 5 • **LACP Role Configuration**

Configuring the Timeout

Timeout controls the period between BPDU transmissions. Fast transmits LACP packets each second while Slow waits for 30 seconds before sending a LACP packet. The default value is Fast.

CLI Example: Set LACP Timeout to slow on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# lacp timeout ?
    fast    Transmit BPDU each second (fast timeout)
    slow    Transmit BPDU each 30th second (slow timeout)
(config-if)# lacp timeout slow
```



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	□	Auto ▾		Active ▾	Fast ▾	32768

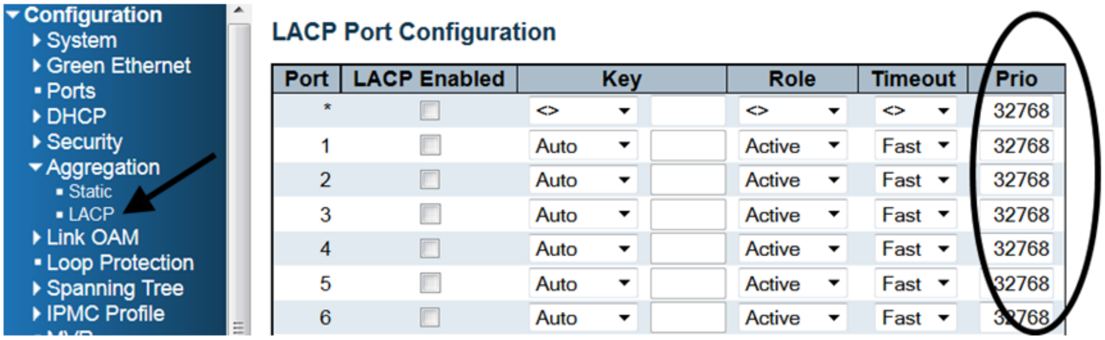
Figure 6 • **LACP Timeout Configuration**

Configuring the Priority

Priority controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device, then this parameter controls which ports will be active and which ports will be in a backup role. Lower numbers mean greater priority. The default value is 32768.

CLI Example: Set LACP priority to 1000 on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# lacp port-priority ?
    <1-65535>    Priority value, lower means higher priority
(config-if)# lacp port-priority 1000
```



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	□	Auto		Active	Fast	32768

Figure 7 **• LACP Priority Configuration**

Showing the Status

The current LACP mode can be viewed with the show lacp command, as follows:

```
# show lacp ?
    internal       Internal LACP configuration
    neighbour      Neighbour LACP status
    statistics     Internal LACP statistics
    system-id      LACP system id
```

MAC Address Table

Switching is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to. This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

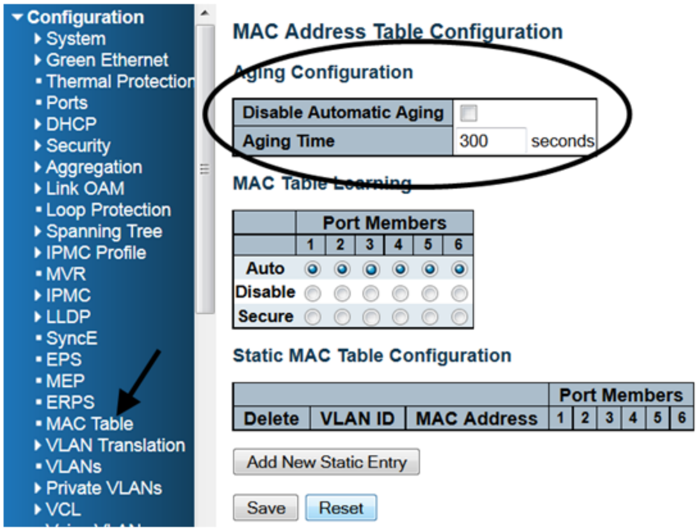
The frames also contain a source MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time.

Setting the Aging Time

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is called aging.

CLI Example: Change the aging time to 600 seconds

```
# configure terminal
(config)#
(config)# mac address-table aging-time ?
    <0,10-1000000>    Aging time in seconds, 0 disables aging
(config)# mac address-table aging-time 600
```



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

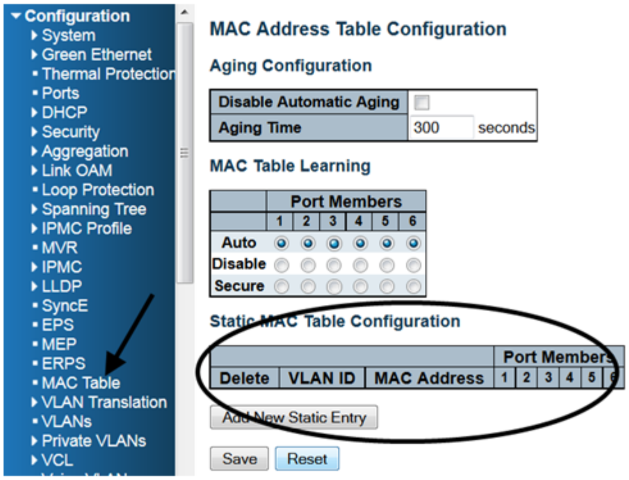
Figure 8 • **MAC Address Table Aging Configuration**

Adding a Static MAC Address Entry

CLI Example: Add the static MAC address: 00:00:00:00:00:01 in VLAN 2 on the first Gigabit port

```
# configure terminal
(config)#
(config)# mac address-table ?
    aging-time    Mac address aging time
    static        Static MAC address
```

```
(config)# mac address-table static 00:00:00:00:00:01 vlan 2 interface
GigabitEthernet 1/1
```



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

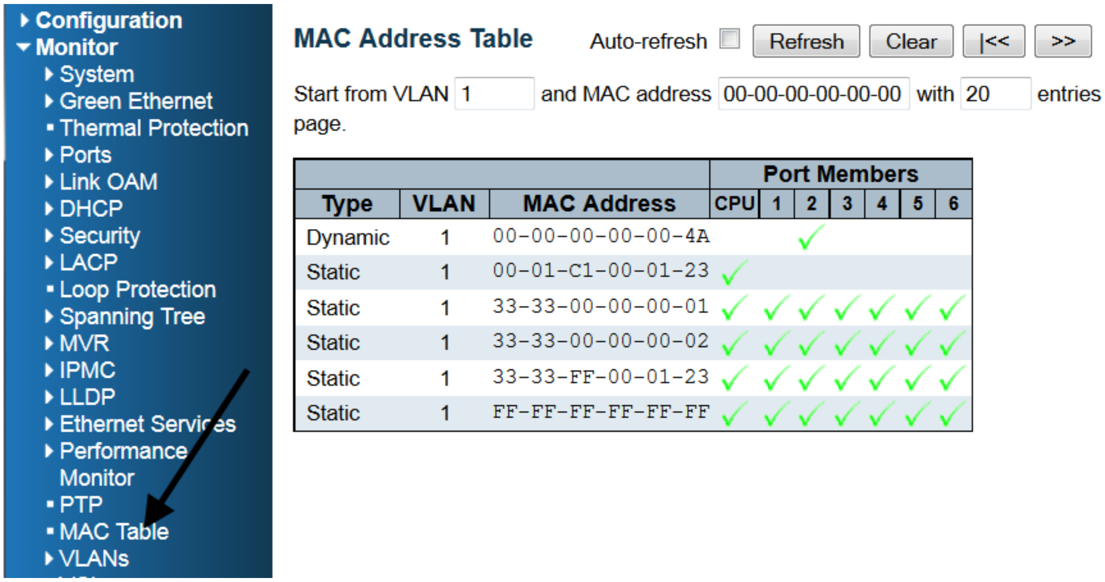
			Port Members					
Delete	VLAN ID	MAC Address	1	2	3	4	5	6

Figure 9 • **Static MAC Address Configuration**

Showing the MAC Address Table

The current MAC address table can be viewed with the show mac address-table command as follows:

```
# show mac address-table
```



MAC Address Table

Auto-refresh □

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	00-00-00-00-00-4A			✓				
Static	1	00-01-C1-00-01-23	✓						
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-00-01-23	✓	✓	✓	✓	✓	✓	✓
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓

Figure 10 • **MAC Address Table**

VLAN

The following illustration shows an example VLAN configuration.

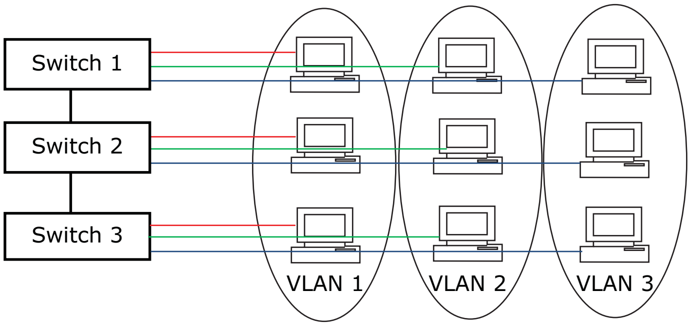


***Figure 11* • VLAN Quick Configuration Example**

Because VLAN 1 is created by default, one need only add VLAN 2 and 3, as follows:

```
# configure terminal
(config)# vlan 2
(config)# vlan 3
```

Set the access port. Assume that port 1 through3 are connected to the PC. The PVID of each port is different.

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode access
(config-if)# switchport access vlan 1
(config)# exit
(config)# interface GigabitEthernet 1/2
(config-if)# switchport mode access
(config-if)# switchport access vlan 2
(config)# exit
(config)# interface GigabitEthernet 1/3
(config-if)# switchport mode access
(config-if)# switchport access vlan 3
(config)# exit
```

Set the trunk port. Assume that port 4 is connected to the other switch. Set the allowed VLAN to accept 1-3.

```
# configure terminal
(config)# interface GigabitEthernet 1/4
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 1-3
Configure the port such that frames are always transmitted with a tag on port 4.
(config-if)# switchport trunk vlan tag native
```

Global Configuration

Existing VLAN

CLI Example: Adding VLAN 2

```
# configure terminal
(config)# vlan 2
```

CLI Example: Removing VLAN 2

```
# configure terminal
(config)# no vlan 2
```

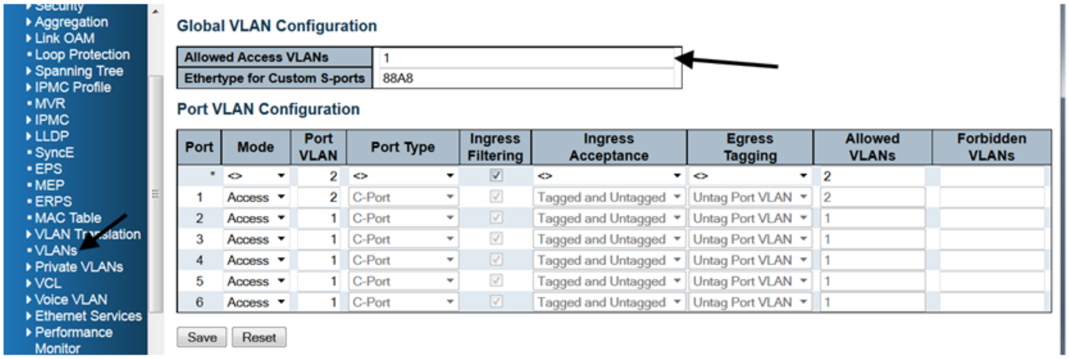
CLI Example: Show existing VLANs

```
# show vlan brief
VLAN  Name                              Interfaces
----  --------------------------------  ----------
1     default                           Gi 1/1-6
2     VLAN0002
```

The Allowed Access VLAN field 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 the following list syntax.

```
# configure terminal
(config)# vlan1,10-13,200,300
```

Individual elements are separated by commas and ranges are specified with a dash separating the lower and upper bound. Spaces are allowed in between the delimiters. The example creates VLANs 1, 10, 11, 12, 13, 200, and 300.



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
*	<>	2	<>	☑	<>	<>	2	
1	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

Figure 12 • **VLAN Allowed Access VLANs Configuration**

VLAN Naming

CLI Example: Set VLAN2's name to test

```
# configure terminal
(config)# vlan 2
(config-vlan)# name test
```

Web GUI

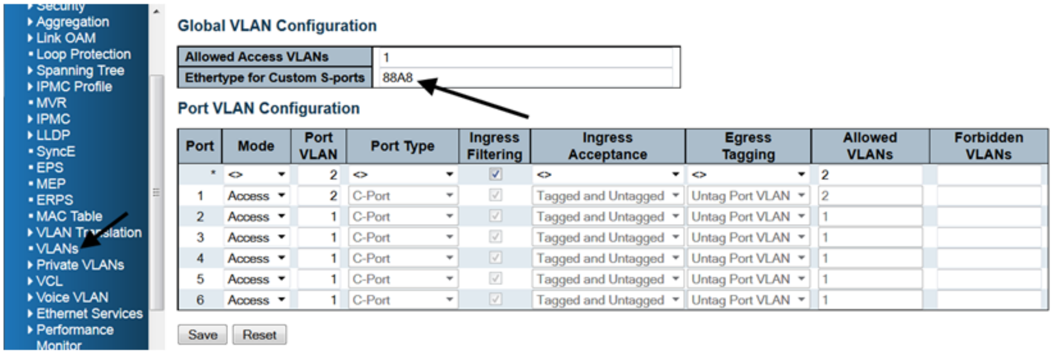
Not available.

Ethertype for Custom S-ports

This field specifies the Ethertype/TPID (specified in hexadecimal) of tagged frames. The setting applies to all ports whose Port Type is set to S-Custom-Port. It takes effect on the egress side.

CLI Example

```
# configure terminal
(config)# vlan ethertype s-custom-port
<0x0600-0xffff>
```



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
*	<>	2	<>	☑	<>	<>	2	
1	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

***Figure 13* • VLAN Ethertype for Custom S-ports Configuration**

Port Based Configuration

Port Mode

Port mode determines the fundamental behavior of the port in question. A port can be in one of three modes, with Access being the default.

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 LAN or 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
- Upon 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:

- Member of all existing VLANs by default (limited by the use of allowed VLANs)
- All frames except those classified to the Port VLAN or Native VLAN get tagged on egress by default (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 while including additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have the following 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

CLI Example: Configure as Access port on the first Gigabit port

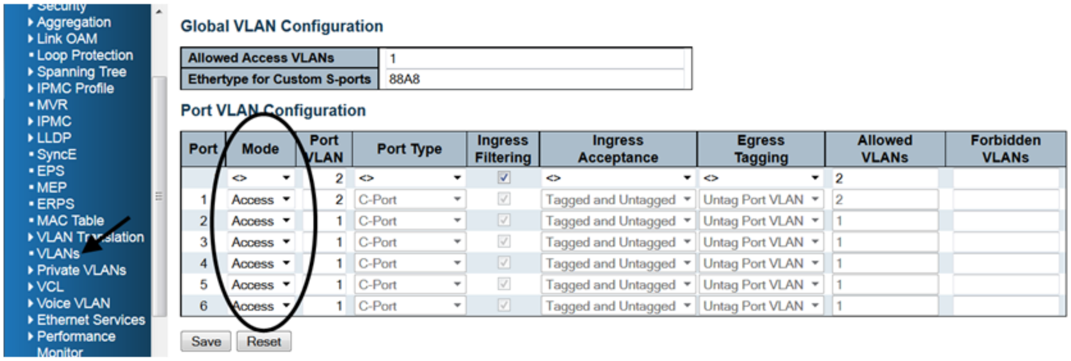
```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode access
```

CLI Example: Configure as Trunk port on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode trunk
```

CLI Example: Configure as Hybrid port on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode hybrid
```



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
	<>	2	<>	☑	<>	<>	2	
1	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

Figure 14 • **VLAN Mode Configuration**

Port VLAN

Port VLAN determines the port's VLAN ID, or PVID. Allowed VLANs are in the range of 1 through 4095, with the 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 is set to untag port VLAN.

Port VLAN is called an Access VLAN for ports in access mode and Native VLAN for ports in trunk or hybrid mode.

CLI Example: Set Port VLAN to 2 on the first Gigabit port (configured as access mode)

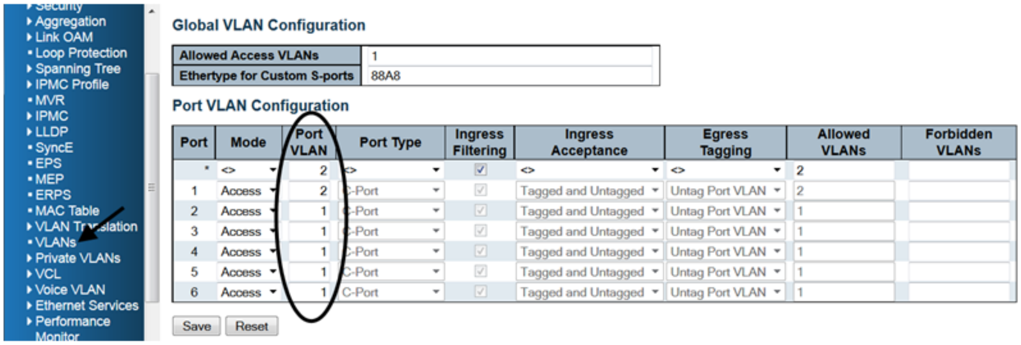
```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport access vlan 2
    <vlan_id>    VLAN ID of the native VLAN when this port is in trunk mode
```

CLI Example: Set Port VLAN to 2 on the first Gigabit port (configured as trunk mode)

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport trunk native vlan 2
```

CLI Example: Set Port VLAN to 2 on the first Gigabit port (configured as hybrid mode)

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport hybrid native vlan 2
```



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
*	<>	2	<>	☑	<>	<>	2	
1	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

Figure 15 • **VLAN PVID Configuration**

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 are tagged with a C-tag.

S-Port

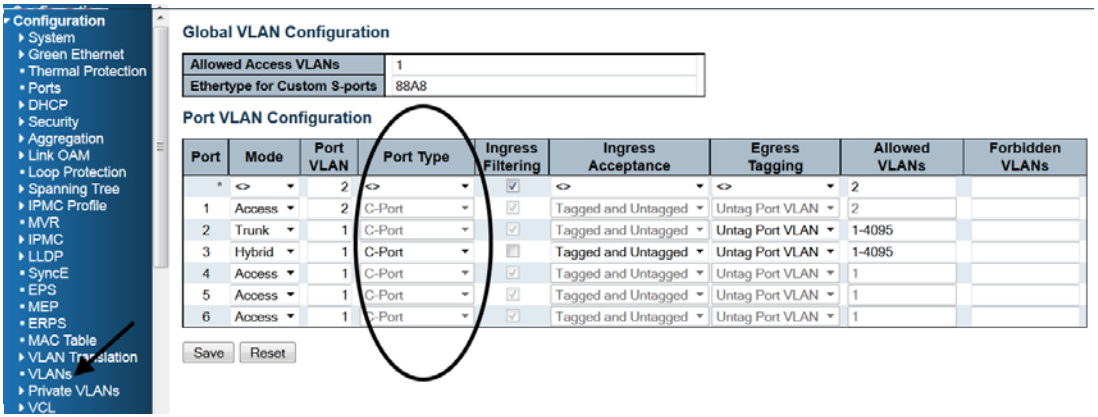
On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.

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.

CLI Example: Set Port Type on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport hybrid port-type ?
    c-port            Customer port
    s-custom-port     Custom Provider port
    s-port            Provider port
    unaware           Port in not aware of VLAN tags
```



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
*	<>	2	<>	☑	<>	<>	2	
1	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	
2	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	
3	Hybrid	1	C-Port	□	Tagged and Untagged	Untag Port VLAN	1-4095	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

Figure 16 **• VLAN Port Type Configuration**

Ingress Filtering

Hybrid ports allow for changing ingress filtering. Access and trunk ports always have ingress filtering enabled.

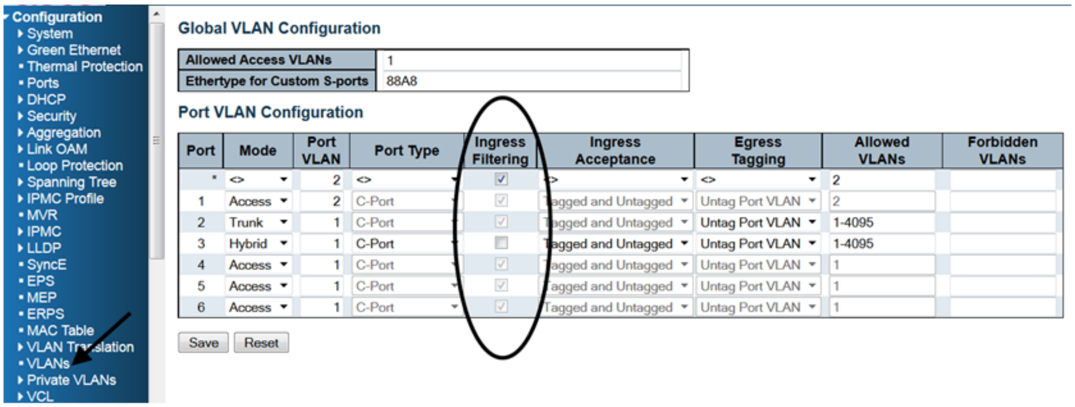
If ingress filtering is enabled, frames classified to a VLAN that the port is not a member of get discarded.

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.

CLI Example: Set ingress filtering on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport hybrid ?
    acceptable-frame-type    Set acceptable frame type on a port
    allowed                  Set allowed VLAN characteristics when interface
is in hybrid mode
    egress-tag               Egress VLAN tagging configuration
    ingress-filtering        VLAN Ingress filter configuration
```

native	Set native VLAN	port-type	Set port type



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
*	<>	2	<>	☑	<>	<>	2	
1	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	
2	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	
3	Hybrid	1	C-Port	☐	Tagged and Untagged	Untag Port VLAN	1-4095	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

Figure 17 • **VLAN Ingress Filtering Configuration**

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

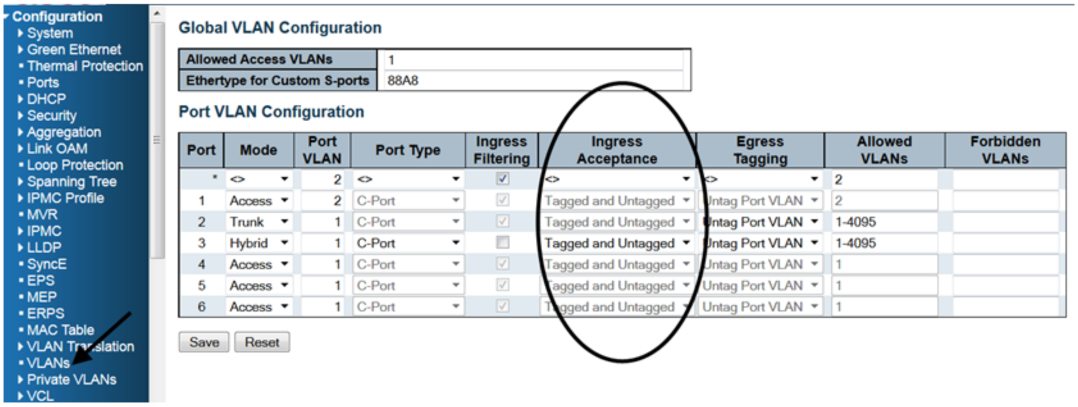
Only tagged frames are accepted on ingress. Untagged frames are discarded.

Untagged Only

Only untagged frames are accepted on ingress. Tagged frames are discarded.

CLI Example: Configure ingress filtering on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport hybrid acceptable-frame-type ?
    all         Allow all frames
    tagged      Allow only tagged frames
    untagged     Allow only untagged frames
```



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
*	<>	2	<>	☑	<>	<>	2	
1	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	
2	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	
3	Hybrid	1	C-Port	☐	Tagged and Untagged	Untag Port VLAN	1-4095	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

Figure 18 **• VLAN Ingress Acceptance Configuration**

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.

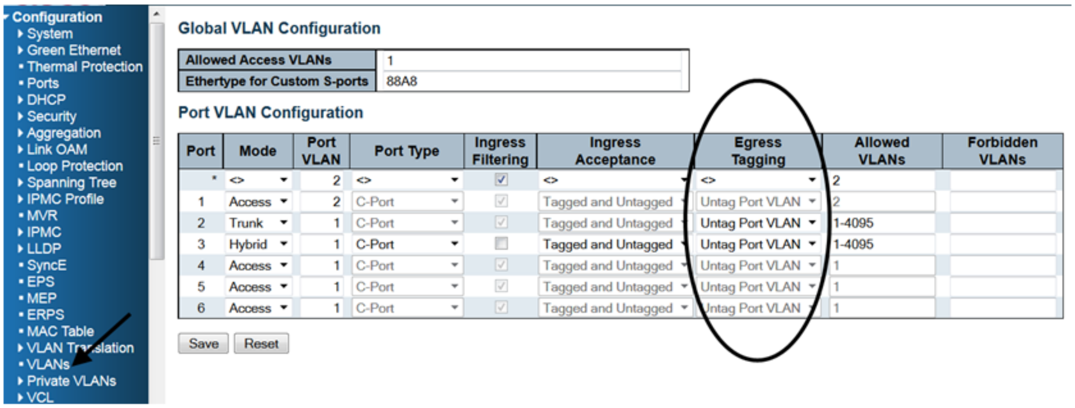
Untag All

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.

CLI Example: Set egress tagging on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport hybrid egress-tag ?
    all     Tag all frames
```

```
        none      No egress tagging
```



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
*	<>	2	<>	☑	<>	<>	2	
1	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	
2	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	
3	Hybrid	1	C-Port	☐	Tagged and Untagged	Untag Port VLAN	1-4095	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

Figure 19 **• VLAN Egress Tagging Configuration**

Allowed VLANs

Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be members of the Access VLAN.

The field's syntax is identical to the syntax used in the Existing VLANs field. By default, a port may become a member of all possible VLANs, and is therefore set to 1-4095.

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

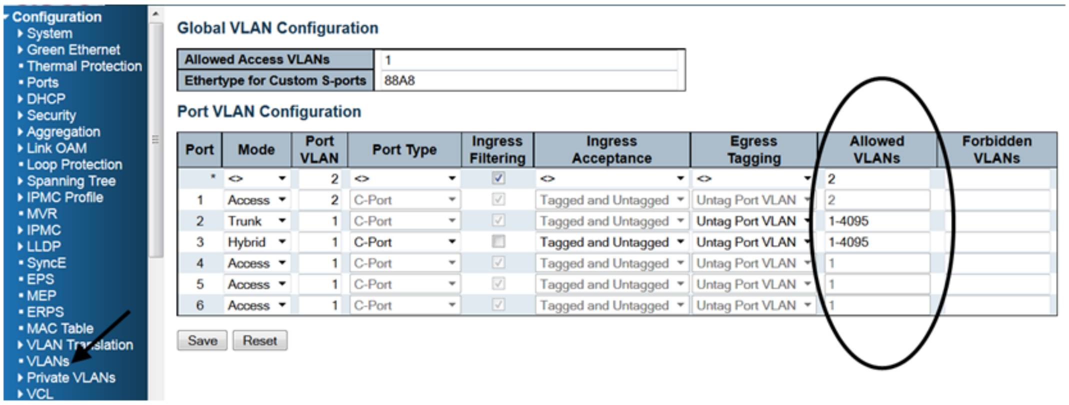
CLI Example: Set port VLAN to 2 on the first Gigabit port (configured as trunk mode)

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport trunk allowed vlan ?
   <vlan_list>   VLAN IDs of the allowed VLANs when this port is in hybrid mode
    add            Add VLANs to the current list
    all            All VLANs
    except         All VLANs except the following
    none           No VLANs
    remove         Remove VLANs from the current list
```

CLI Example: Set port VLAN to 2 on the first Gigabit port (configured as hybrid mode)

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport hybrid allowed vlan ?
   <vlan_list>   VLAN IDs of the allowed VLANs when this port is in hybrid mode
    add            Add VLANs to the current list
    all            All VLANs
    except         All VLANs except the following
    none           No VLANs
```

```
            remove          Remove VLANs from the current list
```



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
*	<>	2	<>	☑	<>	<>	2	
1	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	
2	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	
3	Hybrid	1	C-Port	☐	Tagged and Untagged	Untag Port VLAN	1-4095	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

Figure 20 • **Allowed VLANs Configuration**

Forbidden VLANs

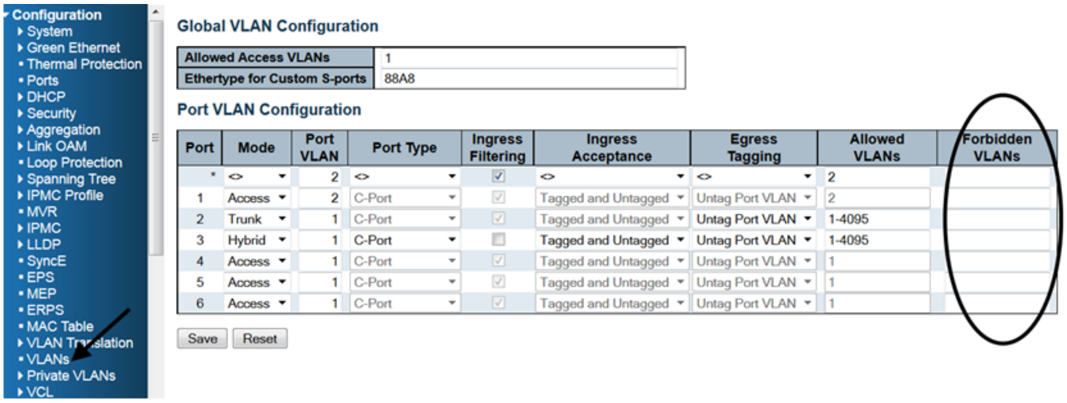
A port may be configured to never be a member of one or more VLANs. This is particularly useful when dynamic VLAN protocols such as MVRP and GVRP must be prevented from dynamically adding ports to VLANs.

The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Existing VLANs field.

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

CLI Example: Configure forbidden VLAN on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport forbidden vlan ?
    add        Add to existing list.
    remove     Remove from existing list.
```



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
*	<>	2	<>	☑	<>	<>	2	
1	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	
2	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	
3	Hybrid	1	C-Port	☐	Tagged and Untagged	Untag Port VLAN	1-4095	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

Figure 21 • **Forbidden VLANs Configuration**

Show VLAN Status

CLI Example

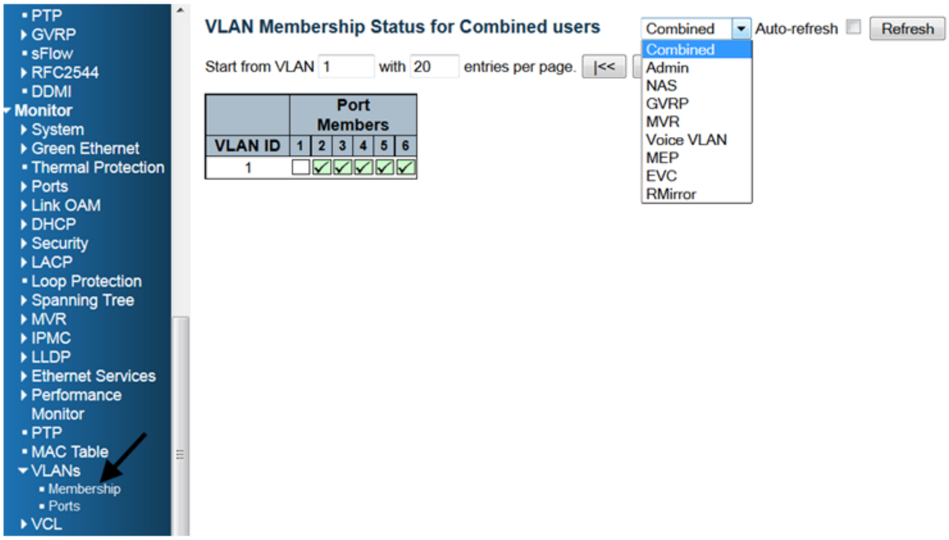
```
# show vlan ?
    brief         VLAN summary information
    id            VLAN status by VLAN id
    ip-subnet     Show VLAN ip-subnet entries.
    mac           Show VLAN MAC entries.
    name          VLAN status by VLAN name
    protocol      Protocol-based VLAN status
    status        Show the VLANs configured for each interface.
    <cr>
```

Web GUI

Various internal software modules may use VLAN services to configure VLAN memberships such as NAS, GVRP, MVR, Voice VLAN, MEP, or EVC.

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 module configuration to reflect what is actually configured in hardware.



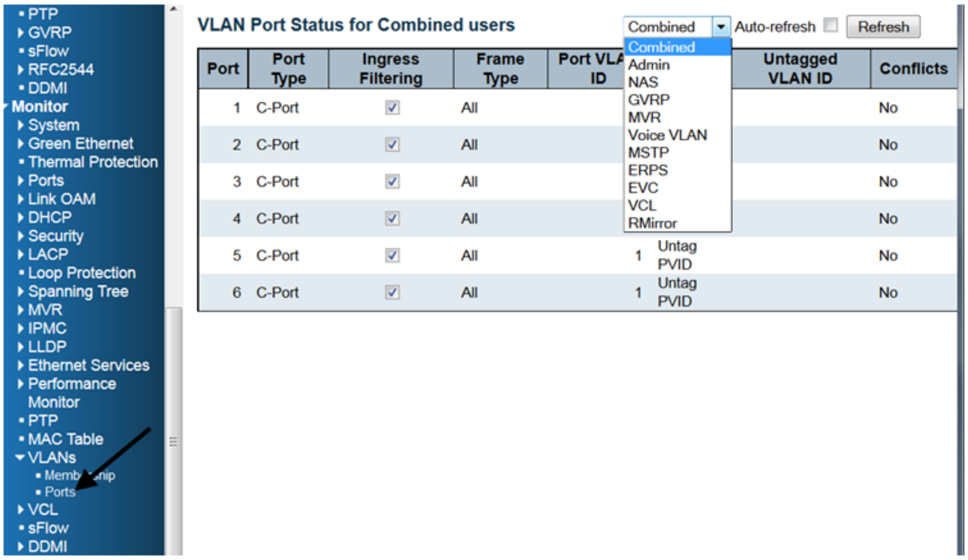
VLAN Membership Status for Combined users

Combined ▾ Auto-refresh □ Refresh

Start from VLAN 1 with 20 entries per page. |<<

	Port Members					
VLAN ID	1	2	3	4	5	6
1	□	✓	✓	✓	✓	✓

Figure 22 • **VLAN Membership Status**



VLAN Port Status for Combined users

Port	Port Type	Ingress Filtering	Frame Type	Port VLA ID		Untagged VLAN ID	Conflicts
1	C-Port	☑	All				No
2	C-Port	☑	All				No
3	C-Port	☑	All				No
4	C-Port	☑	All				No
5	C-Port	☑	All	1	Untag PVID		No
6	C-Port	☑	All	1	Untag PVID		No

Figure 23 **• VLAN Port Status**

Mirroring and Remote Mirroring

Local Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port.

Mirror the Traffic of Port X to Port Y

1. Enable Mirror session

```
# configure terminal
(config)# monitor session 1
```

2. Mirror the traffic (both rx and tx) of the first Gigabit port

```
(config)# monitor session 1 source interface GigabitEthernet 1/1 both
```

3. Configure the mirror destination port to Gigabit port 6

```
(config)# monitor session 1 destination interface GigabitEthernet 1/6
```

4. Verify the monitor setting

```
(config)# end
# show monitor session 1
Session 1
---------
Mode                     : Enabled
Type                     : Mirror
Source VLAN(s)           :
Source Ports             :
    Both                 : 1/1
Destination Ports        : 1/6
Disable Mirror session
# configure terminal
(config)# no monitor session 1
```

Mirror the Traffic of VLAN N to Port Y

1. Enable Mirror session

```
# configure terminal
(config)# monitor session 1
```

2. Mirror the traffic of VLAN 123

```
(config)# monitor session 1 source vlan 123
```

3. Configure the mirror destination port to Gigabit port 6

```
(config)# monitor session 1 destination interface GigabitEthernet 1/6
```

Remote Mirroring

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

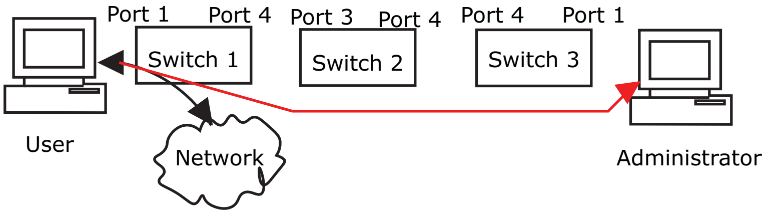


Figure 24 • **Remote Mirroring**

Switch 1

Configure switch 1 as the source switch with the following parameters

- Source port: 1
- Mirror mode: both, frames received and frames transmitted are mirrored.
- Intermediate port: 4

Note: The intermediate port needs to disable MAC table learning.

- VLAN for mirrored traffic: 200

CLI Example: Remote mirroring - source switch configuration

```
# configure terminal
(config)# monitor session 1
(config)# monitor session 1 source interface GigabitEthernet 1/1 both
(config)# monitor session 1 intermediate interface GigabitEthernet 1/4
(config)# monitor session 1 destination remote vlan 200
(config)# interface GigabitEthernet 1/2
(config-if)# no spanning-tree
(config-if)# no mac address-table learning
```

Switch 2

Configure switch 2 as Intermediate switch with the following parameters.

- Intermediate port: 3 and 4

Note: The intermediate port needs to disable MAC Table learning.

- VLAN for mirrored traffic: 200

CLI Example: Remote mirroring - intermediate switch configuration

```
# configure terminal
(config)# monitor session 1
(config)# monitor session 1 intermediate interface GigabitEthernet 1/3-4
(config)# monitor session 1 intermediate remote vlan 200
(config)# interface GigabitEthernet 1/3-4
(config-if)# no mac address-table learning
```

Switch 3

Configure switch 3 as the destination switch with the following parameters.

- Intermediate port: 4

Note: The intermediate port needs to disable MAC Table learning.

- Destination port: 1

Note: The device only supports one destination port.

Note: The destination port needs to disable MAC Table learning.

- VLAN for mirrored traffic: 200

CLI Example: Remote mirroring - destination switch

```
# configure terminal
(config)# monitor session 1
(config)# monitor session 1 destination interface GigabitEthernet 1/1
(config)# monitor session 1 intermediate interface GigabitEthernet 1/4
(config)# monitor session 1 source remote vlan 200
(config)# interface GigabitEthernet 1/1,4
(config-if)# no mac address-table learning
```

Configuration Options

Type

Mirror

Configure the switch to local mirror mode. The source port(s) and destination port are located on the same switch.

Source

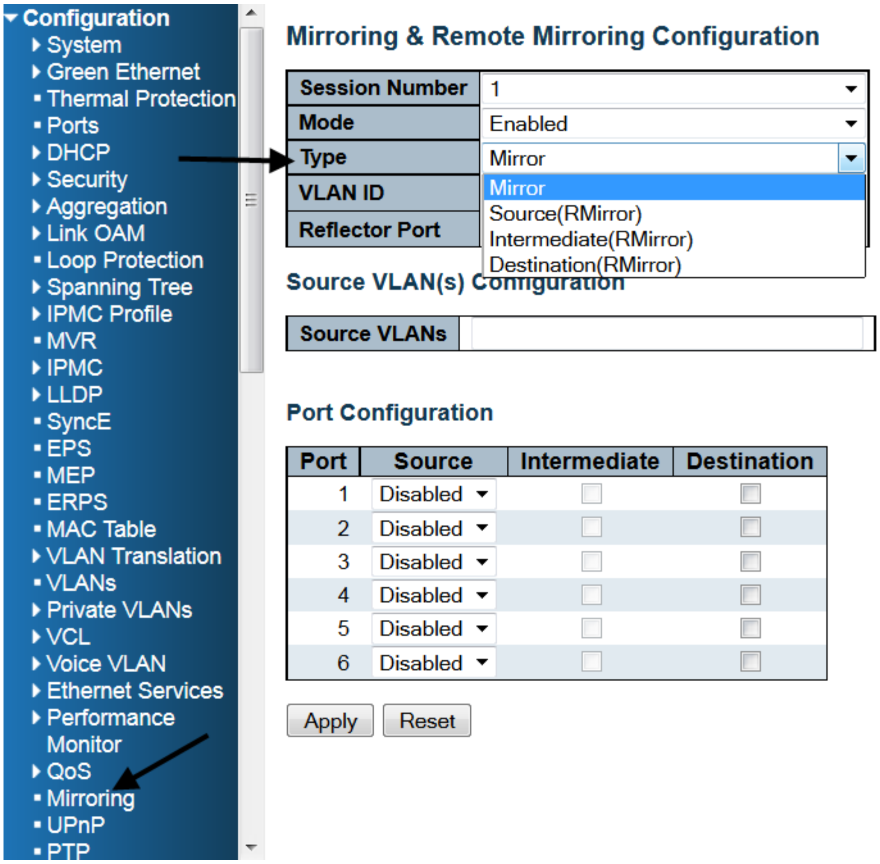
Configure the switch as a source node for monitor flow. The source port(s), and intermediate port(s) are located on this switch.

Intermediate

Configure the switch as 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

Configure the switch as an end node for monitor flow. The destination port(s) and intermediate port(s) are located on this switch.



Mirroring & Remote Mirroring Configuration

Session Number	1
Mode	Enabled
Type	Mirror
VLAN ID	
Reflector Port	

Source VLAN(s) Configuration

Source VLANs	

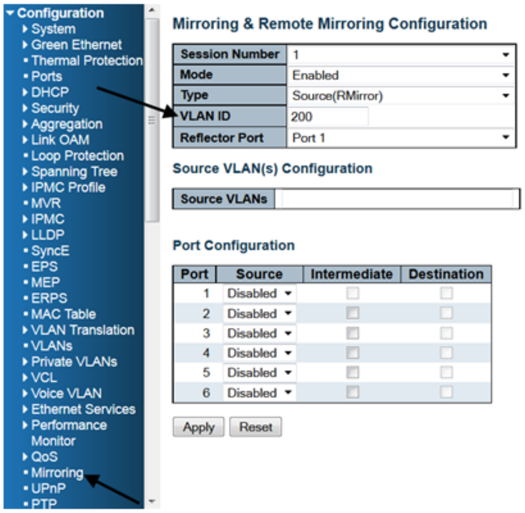
Port Configuration

Port	Source	Intermediate	Destination
1	Disabled	□	□
2	Disabled	□	□
3	Disabled	□	□
4	Disabled	□	□
5	Disabled	□	□
6	Disabled	□	□

Figure 25 • **Mirroring Type**

VLAN ID

The VLAN ID points out where the monitor packet will copy to. It is recommend to be separate from the VLAN of normal data traffic.



Mirroring & Remote Mirroring Configuration

Session Number	1
Mode	Enabled
Type	Source(RMirror)
VLAN ID	200
Reflector Port	Port 1

Source VLAN(s) Configuration

Source VLANs	

Port Configuration

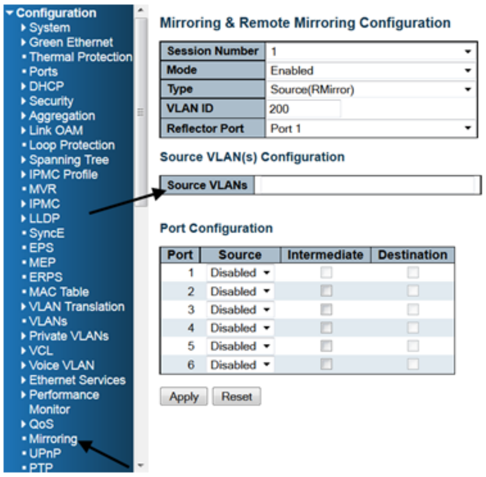
Port	Source	Intermediate	Destination
1	Disabled	□	□
2	Disabled	□	□
3	Disabled	□	□
4	Disabled	□	□
5	Disabled	□	□
6	Disabled	□	□

Figure 26 **• Remote Mirroring- VLAN ID**

Source VLAN(s) Configuration

The switch can support VLAN-based mirroring.

Note: The mirroring session may have either ports or VLANs as sources, but not both.



Mirroring & Remote Mirroring Configuration

Session Number	1
Mode	Enabled
Type	Source(RMirror)
VLAN ID	200
Reflector Port	Port 1

Source VLAN(s) Configuration

Source VLANs	

Port Configuration

Port	Source	Intermediate	Destination
1	Disabled	□	□
2	Disabled	□	□
3	Disabled	□	□
4	Disabled	□	□
5	Disabled	□	□
6	Disabled	□	□

Figure 27 **• Mirroring Source VLAN**

Remote Mirroring Port Configuration

Source

- 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

For remote mirroring only, the intermediate port is a switched port to connect to other switch.

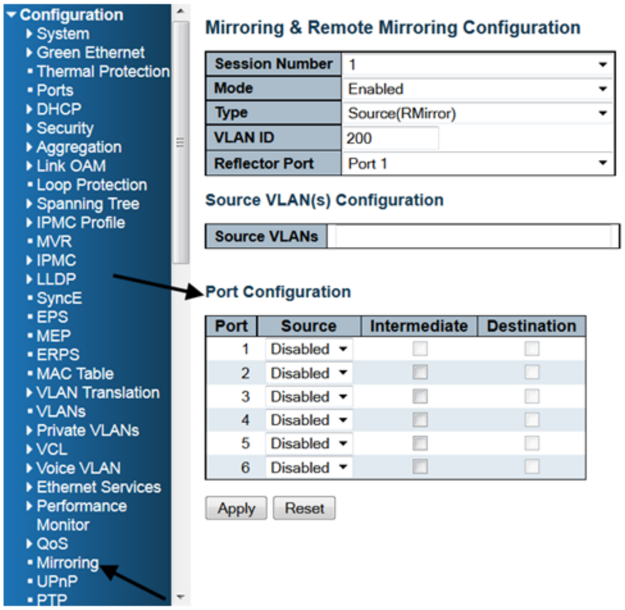
Note: The intermediate port needs to disable MAC table learning.

Destination

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.



Mirroring & Remote Mirroring Configuration

Session Number	1
Mode	Enabled
Type	Source(RMirror)
VLAN ID	200
Reflector Port	Port 1

Source VLAN(s) Configuration

Source VLANs	

Port Configuration

Port	Source	Intermediate	Destination
1	Disabled	□	□
2	Disabled	□	□
3	Disabled	□	□
4	Disabled	□	□
5	Disabled	□	□
6	Disabled	□	□

Figure 28 • **Mirroring Port Configuration**

Configuration Guideline for All Features

When the switch is running in Remote Mirroring mode, the administrator needs to check whether or not other features are enabled or disabled.

The following table lists the recommended settings.

Table 1 • **Configuration Guideline for All Features**

Feature	Impact	Source Port	Intermediate Port	Destination Port	Remote Mirroring VLAN
arp_inspection	High		disabled*		
acl	Critical		disabled*	disabled*	

Table 1 • **Configuration Guideline for All Features**

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			disabled^{o}	
lldp	Low			disabled^{o}	
mac learning	Critical		disabled*	disabled*	
mstp	Critical			disabled^{o}	
mvr	Critical				un-conflict
nas	Critical		authorized*	authorized*	
psec	Critical		disabled*	disabled*	
qos	Critical		unlimited*	unlimited*	
upnp	Low			disabled^{o}	
mac-based vlan	Critical		disabled*		
protocol-based vlan	Critical		disabled*		
vlan_translation	Critical		disabled*	disabled*	
voice_vlan	Critical		disabled*		

* -- must

o -- optional

Impact: Critical/High/Low

Critical	5 packets -> 0 packet
High	5 packets -> 4 packets
Low	5 packets -> 6 packets

GVRP

Generic VLAN Registration Protocol (GVRP) is specified in IEEE 802.1Q-2005, clause 11 and IEEE 802.1D.2004, clause 12.

GVRP Global Configuration

Join-time, Leave-time and LeaveAll-time are protocol parameters in units of centi-seconds, (i.e., in 1/100 seconds). These are parameters according to the GARP (IEEE 802.1D-2004, clause 12) standard.

```
(config)# [no] gvrp time join-time 19
(config)# [no] gvrp time leave-time 61
(config)# [no] gvrp time leave-all-time 1234
```

Where the **no** form disables GVRP or puts the protocol parameter into its default value. The commands can also be put into a single line.

```
(config)# gvrp time join-time 19 leave-time 61 leave-all-time 1234
```

The last parameter is the number of VLANs that GVRP can administer. This puts an upper limit to the number resources that can be used.

Max VLANs is set to 20 when GVRP is enabled globally using the following command.

```
(config)# [no] gvrp
```

If a different value is needed, say 100, enable GVRP using the following command.

```
(config)# gvrp max-vlans 100
```

Note: GVRP must be disabled in advance for the max-vlan number to be changed.

The State of GVRP

It is possible to see what state the GVRP protocol is in with the following command.

```
# _debug_privilege_
#
# debug gvrp protocol-state interface GigabitEthernet 1/* vlan 1-10
|<-------- State of: ------->||<--- Timer [cs]: -->|
Sw Port VLan Applicant Registrar LeaveAll txPDU leave leaveall GIP-Context
1 9 1 VO Fixed Passive - - 137 -
1 9 2 VO MT Passive - - 136 -
1 9 3 VO MT Passive - - 136 -
1 9 4 VO MT Passive - - 135 -
...
1 9 10 VO MT Passive - - 132 -
#
```

In this example we say we will see the state for all gigabit port in switch 1 and VLANs in range 1-10. From the output it turns out, that only port 9 was GVRP enabled. Also see that VLAN ID 1 is Fixed. Only ports that are GVRP enabled are displayed.

All terms like Applicant, Registrar, … , GIP-Context, can be found in the GARP standard.

A dash for a timer means that, that timer is not running. A dash for GIP-Context means that that particular entry is not in a GIP-Context. This will be the case, if the port is down or if it is not in forwarding mode due to spanning tree.

GIP-Context 0 is Base Spanning Tree Context (IEEE 802.1D-2004, 12.2.4). If MSTP is used, then GIP-Context 1 is MSTI-1, …, GIP-Context 7 is MSTI-7.

Multiple Spanning Tree Protocol

Bridge Settings

ICLI Commands for Basic Settings

The following ICLI commands refer to the basic settings.

The *protocol version* is set by the ICLI command:

```
(config)# spanning-tree mode [mstp|rstp|stp]
```

The *bridge priority* is set by:

```
(config)# spanning-tree mst 0 <4096*i, i=0,…,15>
```

where <4096*i, i=0,…,15> is one of the numbers 4096*i, where i=0,…,15.

The *forward delay* is set by:

```
(config)# spanning-tree mst forward-time <4-30>
```

Where <4-30> is one of the numbers 4, 5,…,30.

The *max age* is set by:

```
(config)# spanning-tree mst max-age <6-40>
```

The *max hop* is set by:

```
(config)# spanning-tree mst max-hop <6-40>
```

The *transmit hold count* is set by:

```
(config)# spanning-tree transmit hold-count <1-10>
```

ICLI Commands for Advanced Settings

The following ICLI commands refer to the advanced settings.

The *edge port BPDU filtering* is enabled with the ICLI command:

```
(config)# [no] spanning-tree edge bpdu-filter
```

The *edge port BPDU guard* is enabled with the ICLI command:

```
(config)# [no] spanning-tree edge bpdu-guard
```

The *port error recovery and port error recovery timout* is set by one ICLI command:

```
(config)# [no] spanning-tree recovery interval <30-86400>
```

which both enables and sets the value. The **no** form disables it.

MSTI Configuration

By default, all VLAN Ids are mapped to the Common and Internal Spanning Tree (CIST). If the protocol version is set to MSTP, then a VLAN ID can be mapped to one out of 8 spanning trees, where CIST is one. The 7 others are called MSTI1,…, MSTI7. A MSTI configuration also has a name and revision. All these values have to be identical on the switches in the network. Otherwise the configuration will not take effect.

The configuration identity is configured as follows.

```
(config)# spanning-tree mst name <ConfigurationName> revision <RevisionNumber>
```

where <ConfigurationName> is a string of maximum length 32 characters, and <RevisionNumber> is an integer in the range 1,…,65535.

The VLANs are added to MSTI1 and MIST2 with the following commands.

```
(config)# [no] spanning-tree mst 1 vlan 10-15
(config)# [no] spanning-tree mst 2 vlan 16,18
```

The **no** form deletes all VLANs in the MSTI in question.

MSTI Priorities

Each MSTI and CIST can be given a priority.

A low priority number indicates higher priority.

A *Bridge Identifier* is constructed per CIST, MSTI1,…,MSTI7, the bridge priority number. This is concatenated with the MAC address of the switch. In this way the bridge Identifier is unique.

A low bridge Identifier indicates a higher priority. A high priority means that the switch tends to be the root of the spanning tree. If two switches have the same bridge priority, then for example, setting MSTI1 priority higher, or setting MSTI2 lower, makes one switch tends the root.

STP CIST Port Configuration

STP is configured on a port basis.

All parameters, except *Path Cost* and *Priority*, are specific for the port and not for CIST. These two parameters can be set for each MSTI, but the other parameters cannot because they apply to the port. If, for example, spanning tree is disabled (as it is for port 3), it applies to the CIST and all the MSTIs.

When using the ICLI, the *CIST Aggregation Port Configuration* commands are performed at the *Config* mode prompt as follows.

```
(config)#
```

The *CIST Normal Port Configuration* commands are performed in the *Config Interface* mode prompt as follows.

```
(config-if)#
```

The following commands below assume that the user is in the interface config mode.

STP Enabled

A port can be individually enabled or disabled for taking part in the spanning tree protocol with the following command.

```
(config-if)# [no] spanning-tree
```

Path Cost and Priority

The path cost and priority are set by the following commands:

```
(config-if)# spanning-tree mst 0 cost <Cost>
(config-if)# spanning-tree mst 0 port-priority <Priority>
```

<Cost> is a number in the range 1 to 200000000 or it may be auto. If set to auto, the path cost will be set to some value appropriate for the physical link speed, using IEEE 802.1D recommended values.

<Priority> is a number in the range 0 to 240 and a multiple of 16. If it is not a multiple of 16 then it will be set to 0.

The path cost is used by STP when selecting ports. Low cost is chosen in favor of high cost. If two ports have the same cost, then priority is used as a tie breaker.

Admin Edge and Auto Edge

These two features are activated by the following ICLI commands.

```
(config-if)# [no] spanning-tree edge
(config-if)# [no] spanning-tree auto-edge
```

The first command changes the field *Admin Edge* in the web GUI, and the second changes *Auto Edge*. These two values control how a port is declared to be an edge port or not. An edge port is a port which is not connected to a bridge.

If auto edge is enabled, then the port determines whether it is an edge port by registering if BPDUs are received on that port. The admin edge determines what the port should start as, being edge or not, until auto edge if enabled, then change.

The decision can be seen by selecting **Monitor > Spanning Tree > Bridge Status**, then clicking on CIST. Then the *Edge* field shows the decision.

Restricted Role and Restricted TCN

These two features are activated by the following ICLI commands.

```
(config-if)# [no] spanning-tree restricted-role
(config-if)# [no] spanning-tree restricted-tcn
```

If restricted role is enabled it 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 to 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.

If restricted TCN is enabled it 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.

BPDU Guard

This feature is activatd the following ICLI command.

```
(config-if)# [no] spanning-tree bpdu-guard
```

If enabled it causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the portEdgestatus does not affect this setting.

Point-to-Point

This feature is activated by the following ICLI command.

```
(config-if)# [no] spanning-tree link-type {auto|point-to-point|shared}
```

where the **no** form is equivalent to setting it to auto.

Setting the link to point-to-point, shows up in the web GUI as *Forced True*. Setting it to shared, is shown as *Force False*. Setting it to auto shows as *Auto*.

MSTI Ports

The user must select which MSTI configuration to view starting at **Configuration > Spanning Tree > MSTI Ports**.

Select the desired MSTI and click **Get**.

The ICLI commands for setting the path cost and priority is the same as for CIST, but with the change that the MSTI is not 0 (MSTI0 is CIST), but a number from 1 to 7.

```
(config-if)# spanning-tree mst <MSTI> cost <Cost>
(config-if)# spanning-tree mst <MSTI> port-priority <Priority>
```

Here <MSTI> is the number of the MSTI, from 1 to 7.

The other parameters are the same as in the CIST case.

<Cost> is a number in the range 1 to 200000000 or it may be auto. If set to auto, then the path cost will be set to some value appropriate for the physical link speed, using IEEE 802.1D recommended values.

<Priority> is a number in the range 0 to 240 and a multiple of 16. Note that if it is not a multiple of 16 then it will be set to 0.

The path cost is used by STP when selecting ports. Low cost is chosen in favor of high cost. And if two ports have the same cost, then priority is used as a tie breaker.

LLDP Configuration

This document provides step-by-step guidance on how to use ICLI command to set up LLDP, LLDP-MED, and CDP for discovering connected network equipment managed by a management platform, which may be a computer running an IP-capable operating system such as FeeBSD, Linux, or Windows.

- Using ICLI as the management interface requires a serial console connection between the device and the management platform. No network connection is required to use ICLI, but the terminal emulator software needs to be installed.
- Using the Web GUI as the management interface requires an active network connection accessible to the management platform for a browser using IP communication.

It is also recommended that the intended audience of this document is familiar with IP / HTTP technology and has experience in setting up OS application service.

LLDP, LLDP-MED, and CDP

LLDP is used to exchange information between network equipment by advertising information about themselves to the link partners at each interface. The link partners are called neighbors or remote devices. LLDP is defined in IEEE 802.1AB.

LLDP-MED is an extension to the LLDP standard defined in TIA1057. An LLDP-MED enabled device is capable of conveying its capability and configuration to neighbors to guarantee the consistent attributes for the same media service or application across the network.

CDP is a Cisco proprietary protocol that runs over Layer 2 (the data link layer) to automatically discover and learn about other Cisco devices connected to the network. When CDP awareness is enabled, CDP frames are transformed into LLDP information and added to the neighbor entries table. LLDP will not actively transmit CDP PDUs.

LLDP Operation and Configuration

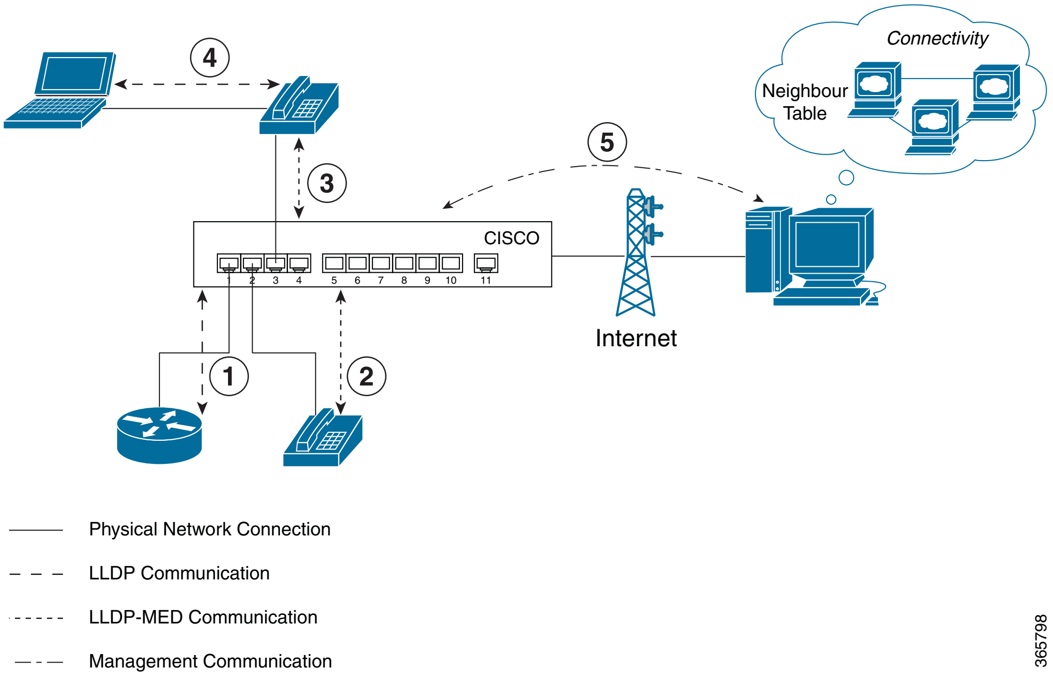
LLDP enables directly connected devices to discover information about each other. It advertises information about the device itself at each interface, allowing other devices in the LAN to learn everything about their peers. Common deployed applications that use the information conveyed by LLDP include the following:

- **Network topology** - Network management system can accurately represent a map of the network topology.
- **Emergency service** - Not only to determine the device location, but also to setup ELIN used for emergency calling. According to the gathered information, public resource coordination for emergency service may also be done.
- **VLAN configuration** - The device can tell the peers which VLAN could be used for streaming services.

- **Power negotiation** - When the device also supports PoE, the connected equipment and the device can negotiate the expected power consumption.

With this capability in the network, automatic device discovery is very helpful for network administration and easy for streaming application deployment. The following figure illustrates the basic concept of an LLDP operation.

Figure 4-1 LLDP Operations



Using LLDP reduces network administration effort by simply connecting the network equipment. In the preceding illustration, one VoIP phone and a laptop are connected in a chain to share the same port on a device that supports LLDP, while another VoIP phone and network equipment are connected to other ports on the same device.

1. When the network equipment is connected, LLDP communication starts and it is recognized as a neighbor that provides networking capability.
2. When the IP phone is connected, LLDP recognizes this neighbor is capable of running VoIP application by exchanging LLDP-MED information. Further, the switch might then be able to reserve power (PoE) if the corresponding setting is configured on both IP phone and switch.
3. LLDP recognizes another IP phone is connected and records its information in neighbor table.
4. When the laptop is connected to the phone, LLDP starts among laptop and phone and switch at the same time, even they may not be physically adjacent.
5. The management system, from either local or remote connection, can now query the device to explore the actual network topology.

LLDP also provides the configurable parameters used for transmitting LLDP PDU, which contains multiple TLVs. The following table shows the basic LLDP parameters and their corresponding descriptions.

Table 1 **• LLDP parameters**

Parameter	Description
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 this value, in 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.
Tx Delay	If the system configuration is changed (e.g. 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 ¼ of the Tx Interval value.
Tx Re-Initialization	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 isn't valid anymore. Tx Re-Initialization controls the amount of seconds between the shutdown frame and a new LLDP initialization.
Port Description	Optional TLV: Port description will be included in LLDP information transmitted.
System Name	Optional TLV: System name will be included in LLDP information transmitted.
System Description	Optional TLV: System description will be included in LLDP information transmitted.
System Capability	Optional TLV: System capability will be included in LLDP information transmitted.
Management Address	Optional TLV: Management address will be included in LLDP information transmitted.

In addition to the basic system information about the network equipment, the optional information regarding specific application can be distributed by LLDP devices that support "Configuring LLDP-MED" on page 8.

Configuring LLDP

LLDP is enabled by default (doing both Tx and Rx for LLDPDU) on all the switch ports. The LLDP setup is thus limited to making sure that the LLDP parameter and system TLV are configured as expected. The following is a quick summary of the steps.

1. Enable LLDP on the specific port(s).
2. Set up per port LLDP system TLV to be advertised, if necessary.
3. Set up global LLDP Tx parameters, if necessary.
4. Save the configuration, if needed.

The following table shows the default LLDP settings and their configurable value range.

Table 2 **• Default LLDP Settings and Configurable Value Range**

Parameter	Default	Configurable Range
Tx Interval	30 seconds	5 - 32768 seconds
Tx Hold	4 times	2 - 10 times

Table 2 • **Default LLDP Settings and Configurable Value Range (continued)**

Tx Delay	2 seconds	1 - 8192 seconds
Tx Re-Initialization	2 seconds	1 - 10 seconds
Port LLDP Administration	Tx and RX	Tx, Rx, Tx, and Rx, Disabled
Port Tx Port Description	True	True or False
Port Tx System Name	True	True or False
Port Tx System Description	True	True or False
Port Tx System Capability	True	True or False
Port Tx Management Address	True	True or False

LLDP Setup using Web ICLI

The following table shows the steps used to set up LLDP using ICLI.

Table 3 • **LLDP Setup Using ICLI**

Step	Action	Purpose

1	configure terminal
	Example
	`# configure terminal`
	`(config)#`
		Enters global configuration mode.

2	`interface interface-id`
	Example
	`(config)# interface * (config-if)#`
		Specifies the interface for configuring LLDP, and enters interface configuration mode.

3	`lldp transmit`
	Example
	`(config-if)# lldp transmit`
	`(config-if)#`
		Enable/Disable transmission of LLDP frames.

4	`lldp receive`
	Example
	`(config-if)# lldp receive`
	`(config-if)#`
		Enable/Disable decoding of received LLDP frames.

5	`lldp tlv-select {management-address | port-description |`
	`system-capabilities | system-description | system-name}`
	Example
	`(config-if)# lldp tlv-select system-name`
	`(config-if)#`
		Enable/Disable transmission of optional system TLV.

6	`exit`
	Example
	`(config-if)# exit`
	`(config)#`
		Exits from interface configuration mode and returns to global configuration mode.

7	`lldp timer seconds`
	Example
	`(config)# lldp timer 30 (config)#`
		Sets LLDP Tx interval (The time between each LLDP frame transmitted in seconds).

Table 3 • **LLDP Setup Using ICLI (continued)**

Step	Action	Purpose

8	`lldp holdtime seconds`
	Example
	`(config)# lldp holdtime 4 (config)#`
		Sets LLDP hold time (The neighbor switch will discard the LLDP information after hold time multiplied by timer seconds).

9	`lldp transmission-delay seconds`
	Example
	`(config)# lldp transmission-delay 2 (config)#`
		Sets LLDP transmission-delay. LLDP transmission delay (the amount of time that the transmission of LLDP frames will delayed after LLDP configuration has changed) in seconds.

10	`lldp reinit seconds`
	Example
	`(config)# lldp reinit 2 (config)#`
		LLDP Tx re-initialization delay in seconds.

11	`end`
	Example
	`(config)# end`
	`#`
		Returns to privileged EXEC mode.

12	`copy running-config startup-config`
	Example:
	`# copy running-config startup-config`
	`#`
		(Optional)
		Saves settings in the configuration file.

LLDP-MED Operation and Configuration

LLDP-MED provides a device with an additional ability for serving a specific application. Depending on LLDP-MED operation mode per interface, a device acts either as a connectivity device or an endpoint device on the designated port. The difference between working as a network connectivity device or an endpoint device is a matter of initializing the LLDP-MED TLVs transmission. A network connectivity device does not start LLDP-MED TLVs transmission until it has detected an endpoint device as link partner. An endpoint device starts LLDP-MED TLVs transmission at once.

To achieve these related properties, LLDP-MED defines an LLDP-MED fast start interaction between the protocol and the application layers on top of the protocol. 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. To share LLDP-MED information as quickly as possible, 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.

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 is repeated.

LLDP-MED and the LLDP-MED fast start are 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.

The following four major additional abilities are supported by the LLDP-MED.

1. **Capability discovery** - Enables endpoints to determine the capabilities supported by the connected device. It can also be used to indicate type of the connected device (a phone, a switch, a wireless router, etc.).
2. **Location identification discovery** - Enables the network equipment (mainly IP phones) to be aware of its location information that can be used for location based applications, especially the emergency services.

3. **Network policy discovery** - Provides a mechanism for a switch to notify a connected equipment the VLAN ID that the equipment should use. The equipment can plug into any switch, obtain its VLAN ID, and then start communications.
4. **Power discovery** - Enables two direct connected devices to convey power information, when PoE is introduced, because the switch with PoE capability provides power to the connected equipment.

The following table shows the supported location identification optional TLVs for LLDP-MED.

Table 4 • **Supported Location Identification Optional TLVs for LLDP-MED**

Optional TLV	**Description**
ELIN Address	Emergency call service ELIN identifier, which is used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP.
Country Code	The two-letter ISO 3166 country code in capital ASCII letters.
State	National subdivisions (state, canton, region, province, prefecture).
County	County, parish, gun (Japan), district.
City	City, township, shi (Japan).
City District	City division, borough, city district, ward, chou (Japan).
Block (Neighborhood)	Neighborhood, block.
Street	Street.
Street Direction	Leading street direction.
Trailing Street	Trailing street suffix.
Street Suffix	Street suffix.
House No.	House number.
House No. Suffix	House number suffix.
Landmark	Landmark or vanity address.
Additional	Location Info. Additional Location Information.
Name	Name (residence and office occupant).
Zip Code	Postal/zip code.
Building	Building (structure).
Apartment	Unit (Apartment, suite).
Floor	Floor.
Room No.	Room number.
Place Type	Place type.
Postal Community Name	Postal community name.
P.O. Box	Post office box (P.O. BOX).
Additional	CodeAdditional code.

The following table shows the supported network policy optional TLVs for LLDP-MED.

Table 5 • **Supported Network Policy Optional TLVs for LLDP-MED**

Optional TLV	Description
Datum	Specify the geodetic system to be used: WGS84, NAD83/NAVD88 and NAD83/MLLW.
Latitude	Latitude degrees (within 0-90 degrees) in either north of the equator or south of the equator.
Longitude	Longitude degrees (within 0-180 degrees) in either east of the prime meridian or west of the prime meridian.
Altitude	Altitude value based on the altitude type (meter or floor).
ELIN Address	Emergency call service ELIN identifier, which is used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP.
Country Code	The two-letter ISO 3166 country code in capital ASCII letters.
State	National subdivisions (state, canton, region, province, prefecture).
County	County, parish, gun (Japan), district.
City	City, township, shi (Japan).
City District	City division, borough, city district, ward, chou (Japan).
Block (Neighborhood)	Neighborhood, block.
Street	Street.
Street Direction	Leading street direction.
Trailing Street	Trailing street suffix.
Street Suffix	Street suffix.
House No.	House number.
House No. Suffix	House number suffix.
Landmark	Landmark or vanity address.
Additional Location Info.	Additional Location Information.
Name	Name (residence and office occupant).
Zip Code	Postal/zip code.
Building	Building (structure).
Apartment	Unit (Apartment, suite).
Floor	Floor.
Room No.	Room number.
Place Type	Place type.
Postal Community Name	Postal community name.
P.O. Box	Post office box (P.O. BOX).
Additional	CodeAdditional code.

The following table shows the supported network policy optional TLVs for LLDP-MED.

Table 6 • **Supported Network Policy Optional TLVs for LLDP-MED**

Optional TLV	**Description**
Media Application Type	The application types specifically addressed are: Voice, Guest Voice, Softphone Voice, Video Conferencing, Streaming Video and Control / Signaling (conditionally support a separate network policy for the media types above).
VLAN ID	VLAN identifier (VID) for the port as defined in IEEE 802.1Q. It is valid only when policy is using a 'tagged' VLAN.
Tag	Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN.
L2 Priority	802.1p CoS value used to prioritize the specified application.
DCP	DSCP value to be used to provide Diffserv node behavior for the specific application.

A network policy is intended for use with applications that have specific, real-time network policy requirements such as interactive voice and/or video services. It is potentially advertised and associated with multiple sets of application types supported on a given port.

Configuring LLDP-MED

The LLDP-MED defaults support four kinds of discovery options: Capability, Location Identification, Network Policy, and Power. They also default to transmit capabilities, network policy, and location TLVs in LLDP-MED message exchanges. LLDP needs to be enabled to handle protocol messages before setting LLDP-MED. The following is a quick summary of the steps, and it is assumed LLDP is enabled and functional. For information about LLDP configuration, see LLDP-MED Operation and Configuration, page 4-5.

Capability Discovery

1. Enable capability discovery on specific interface(s).
2. Configure per interface LLDP-MED device type, if necessary.
3. Save the configuration, if needed.

Location Identification Discovery

1. Configure fast start repeat count for LLDP-MED.
2. Configure geodetic system settings.
3. Configure ELIN address for emergency service, if necessary.
4. Configure location information settings.
5. Enable location identification discovery on specific interface(s).
6. Setup per interface LLDP-MED device type, if necessary.
7. Save the configuration, if needed.

Network Policy Discovery

1. Create network policy for the expected application type.
2. Associate the created network policy with selected interface(s).

3. Enable network policy discovery on specific interface(s).
4. Configure per interface LLDP-MED device type, if necessary.
5. Save the configuration, if needed.

Power Discovery

PoE has to be enabled to cooperate with LLDP-MED.

1. Enable power discovery on specific interface(s).
2. Save the configuration, if needed.

Default Settings and Configurable Value Range

The following table shows the default LLDP-MED settings and their configurable value range.

Table 7 • **Default LLDP-MED Settings and Configurable Value Range**

Parameter	Default	Configurable Range
Fast Start Repeat Count	4	1 – 10
Transmit TLVs	capabilities & network-policy & location	capabilities, network-policy and location
Map Datum Type	WGS84	WGS84, NAD83/NAVD88 and NAD83/MLLW
Latitude Type	North	North or South
Latitude	0	0.0000 – 90.0000
Longitude Type	East	East or West
Longitude	0	0.0000 – 180.0000
Altitude Type	Meters	Meters or Floors
Altitude	0	-2097151.9 to 2097151.9
ELIN Address	Null String	String in 0 – 25 characters
Country Code	Null String	String in 0 – 2 characters
State	Null String	String in 0 – 250 characters
County	Null String	String in 0 – 250 characters
City	Null String	String in 0 – 250 characters
City District	Null String	String in 0 – 250 characters
Block (Neighborhood)	Null String	String in 0 – 250 characters
Street	Null String	String in 0 – 250 characters
Street Direction	Null String	String in 0 – 250 characters
Trailing Street	Null String	String in 0 – 250 characters
Street Suffix	Null String	String in 0 – 250 characters
House No.	Null String	String in 0 – 250 characters
House No. Suffix	Null String	String in 0 – 250 characters
Landmark	Null String	String in 0 – 250 characters
Additional Location Info.	Null String	String in 0 – 250 characters

Table 7 • **Default LLDP-MED Settings and Configurable Value Range (continued)**

Name	Null String	String in 0 – 250 characters
Zip Code	Null String	String in 0 – 250 characters
Building	Null String	String in 0 – 250 characters
Apartment	Null String	String in 0 – 250 characters
Floor	Null String	String in 0 – 250 characters
Room No.	Null String	String in 0 – 250 characters
Place Type	Null String	String in 0 – 250 characters
Postal Community	Null String	String in 0 – 250 characters
P.O. Box	Null String	String in 0 – 250 characters
Additional Code	Null String	String in 0 – 250 characters
Network Policy ID	N/A	0 – 31
Media Application Type	Voice	voice voice-signaling guest-voice guest-voice- signaling soft phone-voice video-conferencing streaming-video video-signaling
VLAN ID	1	1 – 4095
Tag	Tagged	Tagged or Untagged
L2 Priority	0	0 – 7
DSCP	0	0 – 63
Port MED Device Type	Connectivity	Connectivity or endpoint
Port MED Optional TLV	Capabilities & location & network-policy & poe	Capabilities location network-policy poe
Port Policy List	N/A	Created network policy ID

LLDP-MED Setup using ICLI

The following table shows the steps used to set up LLDP-MED using ICLI.

Table 8 • **Setting up LLDP-MED Using ICLI**

Step	Action	Purpose

1	`configure terminal`
	Example
	`# configure terminal`
	`(config)#`
		Enters global configuration mode.

2	`lldp med fast counts`
	Example
	`(config)# lldp med fast 4 (config)#`
		Specifies the fast start repeat count for LLDP-MED.

Table 8 • **Setting up LLDP-MED Using ICLI (continued)**

<table>
<tr><th>Step</th><th>Action</th><th>Purpose</th></tr>
<tr><td>3</td><td>lldp med datum {nad83-mllw | nad83-navd88 | wgs84}
Example
(config)# lldp med datum wgs84 (config)#</td><td>Specifies the geodetic system type.</td></tr>
<tr><td>4</td><td>lldp med location-tlv
{
elin-addr string |
latitude {north | south} degrees | longitude {east | west} degrees | altitude {meters | floors} values
}
Example
(config)# lldp med location-tlv altitude meters 0
(config)#</td><td>Assign the geographic coordinate value for the device. Also, the ELIN identification could be specified.</td></tr>
<tr><td>5</td><td>lldp med location-tlv civic-addr
{
additional-code string | additional-info string | apartment string |
block string | building string | city string | country string | county string | district string | floor string | house-no string |
house-no-suffix string |
landmark string |
leading-street-direction string |
name string |
p-o-box string |
place-type string |
postal-community-name string |
room-number string |
state string |
street string |
street-suffix string |
trailing-street-suffix string |
zip-code string
}
Example
(config)# lldp med location-tlv civic-addr country TW (config)# lldp med location-tlv civic-addr zip-code 30055 (config)# lldp med location-tlv civic-addr house-no-suffix 23F,
2B (config)#</td><td>Specifies civic location information.</td></tr>
</table>

Table 8 • **Setting up LLDP-MED Using ICLI (continued)**

Step	Action	Purpose

6	`lldp med media-vlan-policy <policy-id>`
	`{`
	`guest-voice | guest-voice-signaling | softphone-voice | streaming-video | video-conferencing | video-signaling | voice | voice-signaling`
	`}`
	`{`
	`untagged | tagged <v_vlan_id> [ l2-priority <v_0_to_7> ]`
	`}`
	`[dscp dscp]`
	Example
	`(config)# lldp med media-vlan-policy 2 voice untagged dscp 62`
		Creates a network policy that can be assigned to an interface for a specific kind of application.

7	`interface interface-id`
	Example
	`(config)# interface 10GigabitEthernet 1/2`
	`(config-if)#`
		Specifies the interface for setting LLDP-MED, and enters interface configuration mode.

8	`lldp med type {connectivity | end-point}`
	Example
	`(config-if)# lldp med type connectivity`
	`(config-if)#`
		Selects either Network Connectivity Device or an
		Endpoint Device as the interface role.

9	`lldp med transmit-tlv {capabilities | location | network-policy`
	`| poe}`
	Example
	`(config-if)# lldp med transmit-tlv capabilities location network-policy poe`
	`(config-if)#`
		Specifies the optional TLVs to be transmitted.

10	`lldp med media-vlan policy-list policy-range`
	Example
	`(config-if)# lldp med`
	`media-vlan policy-list 0-1 (config-if)#`
		Specifies the media policy that an interface will apply.

11	`end`
	Example
	`(config-if)# end`
	`#`
		Returns to privileged EXEC mode.

12	`copy running-config startup-config`
	Example
	`# copy running-config startup-config`
	`#`
		(Optional)
		Saves settings in the configuration file.

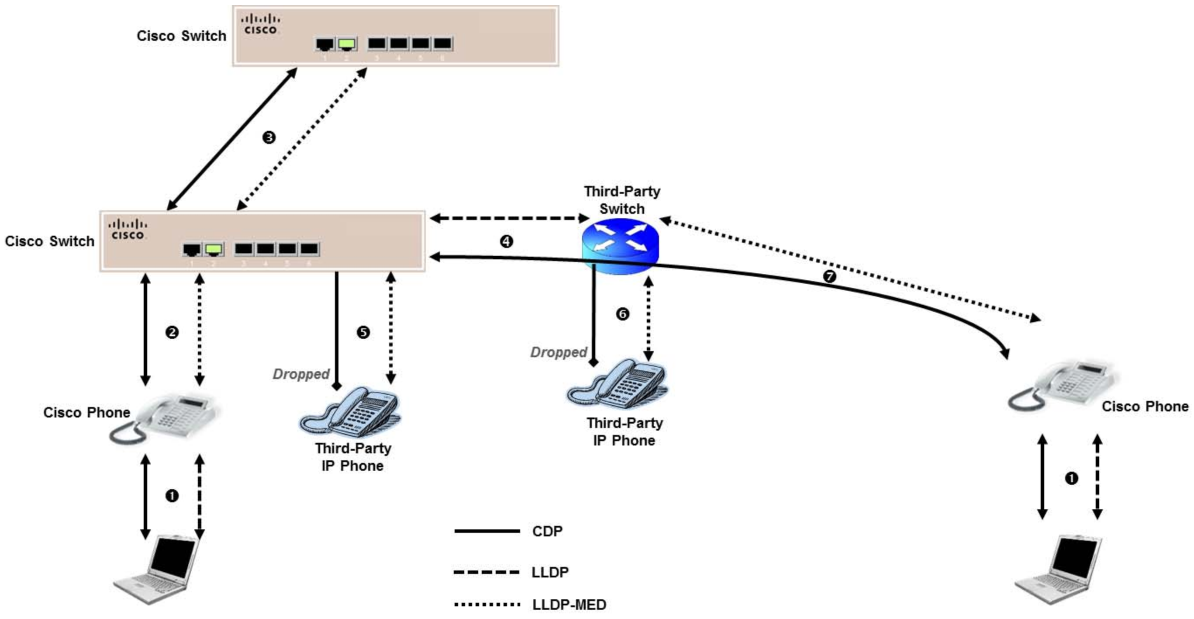
CDP Operation and Configuration

CDP is an L2 proprietary discovery protocol for all Cisco-manufactured devices (routers, bridges, access servers, and switches). It provides the similar concept in using LLDP for network management applications to discover Cisco devices that are neighbors of already known devices. For more information, see Cisco documents for the current CDP capabilities.

LLDP is CDP-aware. It only identifies a Cisco device connected to a device and makes it a neighbor.

The following figure from a Cisco technical white paper illustrates how CDP works.

Figure 4-2 CDP Operations



The following steps describe how CDP works.

1. A laptop connected to a Cisco phone can support CDP. Some applications running on that PC (example Cisco VT Advantage) also support CDP. The Cisco phone therefore uses CDP to support these applications.
2. Both the Cisco switch and the Cisco phone exchange CDP messages.
3. Both Cisco switches exchange CDP and LLDP messages.
4. The Cisco switch exchanges LLDP messages with the third-party switch but still advertises CDP messages. In this case, the third-party switch usually ignores CDP messages and floods the CDP messages to other interfaces, meaning devices connected to the third-party switch receive CDP messages from the Cisco switch as if they are directly connected to the Cisco switch. Cisco recommends turning off CDP on the port connected to the third-party switch that guarantees Cisco application's functionality to a certain extent.
5. A third-party phone drops CDP messages from the Cisco switch but exchanges the LLDP-MED messages with the Cisco switch.
6. A third-party phone drops CDP messages flooded by the third-party switch and only exchanges the LLDP-MED messages with the third-party switch.
7. A Cisco phone generates both CDP and LLDP-MED messages. The third-party switch again ignores CDP messages and floods them out to other interfaces. However, the third-party switch still exchanges LLDP-MED messages with the connected Cisco phone. Again, Cisco recommends turning off CDP on the Cisco switch's port connected to the third-party switch.

Configuring CDP

LLDP is only aware of the existence of Cisco devices upon receiving CDP messages. The CDP operation is restricted to decoding incoming CDP frames, and CDP frames are only decoded if LLDP on the port is enabled.

If all ports have CDP awareness disabled, the device forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled, all CDP frames are terminated by the device.

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 into LLDP neighbors table, as follows:

- 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.

Note: When CDP awareness on an interface is disabled, the CDP information is not removed immediately, but gets removed when the hold time is exceeded.

The following steps summarize the process of configuring CDP.

1. Enable LLDP on the specific interface(s).
2. Enable CDP awareness for the specific interface(s).
3. Save the configuration, if needed.

Default Settings and Configurable Value Range

The following table shows the default CDP settings and their configurable value range.

***Table 9* • Default CDP Settings and Configurable Value Range**

Parameter	Default	Configurable Range
Per Port LLDP Administration	Tx and Rx	Tx, Rx, Tx and Rx, Disabled
CDP Awareness	False	True or False

CDP Setup using ICLI

The following table shows the steps used to set up CDP using ICLI.

***Table 10* • Setting up CDP using ICLI**

Step	Action	Purpose

1	`configure terminal`
	Example
	`# configure terminal`
	`(config)#`
		Enters global configuration mode.

2	`interface interface-id`
	Example
	`(config)# interface * (config-if)#`
		Specifies the interface for enabling LLDP, and enters interface configuration mode.

3	`lldp cdp-aware`
	Example
	`(config-if)# lldp cdp-aware`
	`(config-if)#`
		Specifies if the interface is CDP aware.

Table 10 • **Setting up CDP using ICLI (continued)**

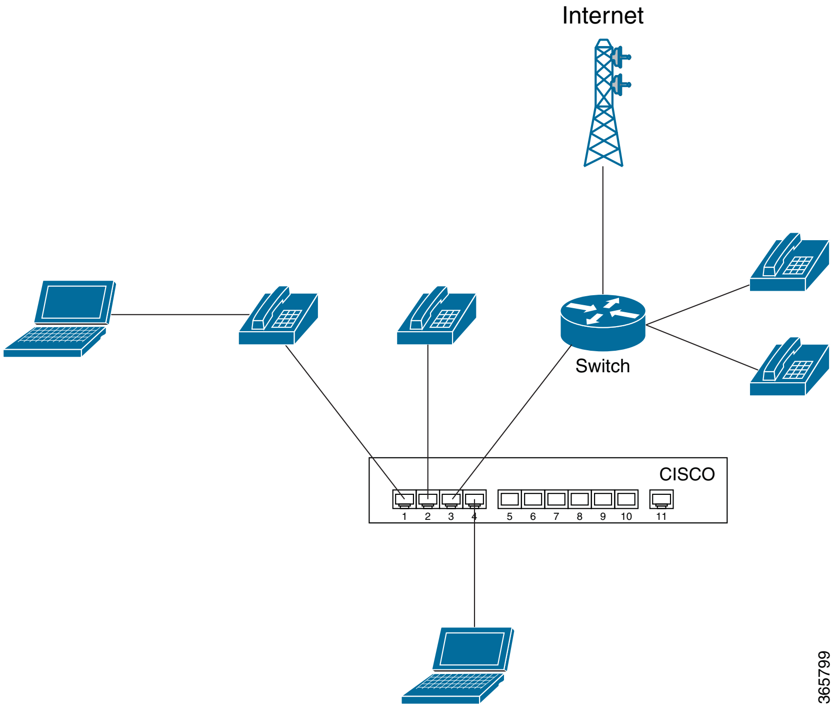
Step	Action	Purpose
4	Example `(config-if)# end`	Returns to privileged EXEC mode.

5	`copy running-config startup-config`
	Example
	`# copy running-config startup-config`
	`#`
		(Optional)
		Saves settings in the configuration file.

Topology Example

The following topology illustration is used to demonstrate the examples, which assume the device boots up with default configurations.

Figure 4-3 Topology Example



Deploy IP Telephony Network using ICLI

The major goal in setting up the IP telephony network is to prioritize the voice data among phones, software, or hardware.

```
# configure terminal
(config)# lldp med media-vlan-policy 0 voice tagged 111 l2-priority 7 dscp 5
(config)# lldp med media-vlan-policy 1 softphone-voice untagged dscp 5
(config)# interface GigabitEthernet 1/1-4
(config-if)# lldp med type connectivity
(config-if)# lldp med transmit-tlv capabilities network-policy
```

```
(config-if)# interface GigabitEthernet 1/1-3 (config-if)# lldp med media-vlan
policy-list 0 (config-if)# interface GigabitEthernet 1/4 (config-if)# lldp med
media-vlan policy-list 1 (config-if)# end
#
```

CHAPTER 5

EVC and OAM Software for Cisco ME1200

This document gives an overview of the software used to support EVC and OAM solutions for ME1200. It includes examples of EVC configurations with associated CLI commands, and describes functionality in ME1200.

Control Modules

The following sections describe the application software control modules and the most important interfaces related to EVC and OAM control.

VLAN Module

The VLAN module is responsible for controlling the VLAN port configuration and VLAN memberships using the following interfaces:

- Consumed Interfaces
  - VLAN APIs
- Provided Interfaces
  - Management APIs for configuration and status
  - Control APIs for dynamic configuration from other modules.

ACL Module

The ACL module is responsible for controlling the ACL port configuration, policer configuration, and ACL rules using the following interfaces:

- Consumed Interfaces
  - ACL APIs
- Provided Interfaces
  - Management APIs for configuration and status
  - Control APIs for dynamic configuration from other modules.

EPS Module

The EPS module controls port protection using the following interfaces:

- Consumed Interfaces
  - EPS APIs
  - MEP module APIs for APS PDU reception and transmission
- Provided Interfaces
  - Management APIs for configuration and status

ERPS Module

The ERPS module controls ring protection using the following interfaces:

- Consumed Interfaces
  - ERPS APIs
  - VLAN module APIs for enabling VLAN ingress filtering
  - MEP module APIs for APS PDU reception and transmission
- Provided Interfaces
  - Management APIs for configuration and status

MEP Module

The MEP module controls the OAM processing using the following interfaces:

- Consumed Interfaces
  - OAM APIs
  - MCE APIs
  - ACL module APIs for CPU copy of frames
  - VLAN module APIs for ERPS management VLAN membership control.
  - EVC module APIs for EVC/ECE change events and configuration access.
- Provided Interfaces
  - Management APIs for configuration and status
  - Control APIs for APS PDU reception and transmission

EVC Module

The EVC module controls and EVC port configuration, policer configuration, EVC/ECE rules and L2CP forwarding using the following APIs:

- Consumed Interfaces
  - EVC APIs
  - Packet APIs
  - VLAN module APIs for EVC VLAN membership control.
- Provided Interfaces
  - Management APIs for configuration and status
  - Control APIs for EVC/ECE change events

EP-Line

Unprotected EP-Line

The following illustration shows a provider network offering an unprotected Ethernet private line between two UNIs. The following sections describe how to configure the edge bridges using CLI commands. It is assumed that the bridges are in default configuration before applying these commands.

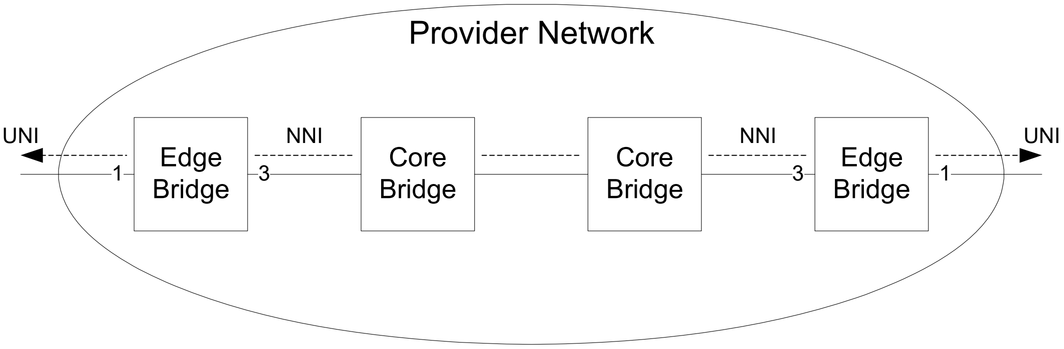


Figure 1 • **Unprotected EP-Line**

Control Protocols

Disable some control protocols that are enabled by default.

```
# Disable STP and LLDP on UNI/NNI ports
interface GigabitEthernet 1/1,3
 no lldp receive
 no lldp transmit
 no spanning-tree
```

VLAN Configuration

Set up the basic VLAN configuration for the UNI and NNI ports.

```
# Exclude UNI/NNI ports from default VLAN
# Set PVID to an unused VLAN to discard non-classified frames
# UNI is C-port, NNI is S-port
interface GigabitEthernet 1/1
 switchport hybrid native vlan 4095
 switchport hybrid allowed vlan none
 switchport hybrid port-type c-port
 switchport mode hybrid
interface GigabitEthernet 1/3
 switchport hybrid native vlan 4095
 switchport hybrid allowed vlan none
 switchport hybrid port-type s-port
 switchport mode hybrid
```

QoS Configuration

Enable one-to-one ingress and egress mapping between CoS and PCP on the UNI and NNI ports.

```
# On UNI and NNI, enable ingress one-to-one mapping from PCP to CoS
interface GigabitEthernet 1/1,3
qos trust tag
 qos map tag-cos pcp 0 dei 0 cos 0 dpl 0
 qos map tag-cos pcp 0 dei 1 cos 0 dpl 1
 qos map tag-cos pcp 1 dei 0 cos 1 dpl 0
 qos map tag-cos pcp 1 dei 1 cos 1 dpl 1
# On UNI and NNI, enable egress one-to-one mapping from CoS to PCP
qos tag-remark mapped
 qos map cos-tag cos 0 dpl 0 pcp 0 dei 0
 qos map cos-tag cos 0 dpl 1 pcp 0 dei 1
 qos map cos-tag cos 1 dpl 0 pcp 1 dei 0
 qos map cos-tag cos 1 dpl 1 pcp 1 dei 1
```

L2CP Configuration

Tunnel all L2 control protocols except LLDP over the EVC. LLDP uses DMAC 01-80-C2-00-00-0E corresponding to L2CP ID 14.

```
# On UNI/NNI port, forward all L2CP except LLDP
interface GigabitEthernet 1/1,3
 evc l2cp forward 0-13,15
```

EVC Configuration

To conserve resources, set up the UNI and NNI ports to use quarter rules in IS1. The EVC is set up with EVC ID 10 and S-VID 1000. The EVC control module will dynamically register VLAN membership for UNI and NNI ports.

```
# Use quarter rules for UNI and NNI
interface GigabitEthernet 1/1,3
 evc key double-tag
# Add EVC 10 using S-VID 1000 and NNI port, disable learning.
evc 10 vid 1000 ivid 1000 interface GigabitEthernet 1/3
```

ECE Configuration

Use ECE rules to divide the UNI traffic into two service classes:

- Frames received on the UNI port with PCP 4-7 values are mapped to class 4 and sent with PCP 4 in the outer tag on the NNI port.
- Other frames received on the UNI port are mapped to class 0 and sent with PCP 0 in the outer tag on the NNI port.

The following sections describe two ways to do this. The first method requires fewer resources.

- Simple NNI: All EVCs on the NNI port are using the same QoS mapping and statistics.
- Advanced NNI: Each EVC on the NNI port has separate QoS mapping and statistics.

Simple NNI

Set up the ECE rules mapping to the EVC.

```
# On UNI port, map tagged frames with PCP 4-7 to class 4, use VID egress lookup
```

```
evc ece 1 interface GigabitEthernet 1/1 outer-tag match type tagged pcp 4-7
add pcp-mode mapped dei-mode dp tx-lookup vid evc 10 cos 4
# On UNI port, map other frames to class 0, with Rx rule only.
evc ece 2 outer-tag add pcp-mode mapped dei-mode dp rule-type rx evc 10 cos 0
```

Advanced NNI

Set up the ECE rules including the QoS mappings.

```
# On UNI port, map tagged frames with PCP 4-7 to class 4, use (VID, PCP) lookup
evc ece 1 interface GigabitEthernet 1/1 outer-tag match type tagged pcp 4-7
tx-lookup pcp-vid evc 10 cos 4
# On UNI port, map other frames to class 0, use (VID, PCP) lookup
evc ece 2 interface GigabitEthernet 1/1 tx-lookup pcp-vid evc 10 cos 0
```

OAM Configuration

The following illustration shows the following OAM MEPs in the left Edge Bridge:

- UNI MEP for port level management at the UNI port.
- NNI MEP for port level management at the NNI port.
- EVC Up MEP for EVC level management seen from the UNI side.
- EVC Down MEP for EVC level management seen from the NNI side.

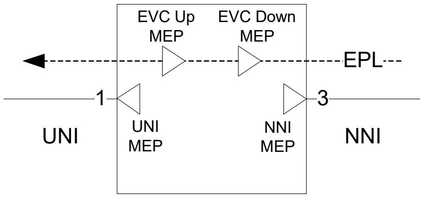


Figure 2 • **Unprotected EP-Line**

The following sections show examples of MEP configurations.

The following commands can be used to create a VOE-based port MEP on the UNI port and enable CCM on this. MEG level 0, MEP ID 1 and peer MEP ID 2 are used. The peer switch must be set up accordingly.

```
# Create UNI port MEP with MEG level 0 and MEP ID 1
mep 1 down domain port flow 1 level 0 interface GigabitEthernet 1/1
mep 1 meg-id ICC000MEG0000 itu mep 1 voe
# Enable UNI peer with MEP ID 2
mep 1 peer-mep-id 2
# Enable CCM on UNI MEP with 1 second interval
mep 1 cc 0
```

NNI MEP

Create a VOE-based port MEP on the NNI port and enable CCM on it.

```
# Create NNI port MEP with MEG level 0 and MEP ID 3
mep 3 down domain port flow 3 level 0 interface GigabitEthernet 1/3
mep 3 meg-id ICC000MEG0000 itu
mep 3 voe
# Enable NNI peer with MEP ID 2
mep 3 peer-mep-id 2
# Enable CCM on UNI MEP with 1 second interval
```

```
mep 3 cc 0
```

EVC Down MEP

Create a VOE-based EVC down MEP on the NNI port and enable CCM on it. MEG level 1, MEP ID 1 and peer MEP ID 2 are used. The peer switch must be set up accordingly. The MEP control module will allocate VOEs and set up MCE rules as needed.

```
# Create EVC Down MEP on NNI port with MEG level 1 and MEP ID 1
mep 10 down domain evc flow 10 level 1 interface GigabitEthernet 1/3
mep 10 meg-id ICC000MEG0000 itu
mep 10 voe
# Enable EVC peer with MEP ID 2
mep 10 peer-mep-id 2
# Enable CCM on EVC MEP with 1 second interval
mep 10 cc 4
```

EVC Up MEP

Create a VOE-based EVC up MEP on the UNI port and enable CCM on it. MEG level 2, MEP ID 1 and peer MEP ID 2 are used. The peer switch must be set up accordingly. The MEP control module will allocate VOEs and set up MCE rules as needed.

```
# Create EVC Up MEP on UNI port with MEG level 2 and MEP ID 1
mep 20 up domain evc flow 10 level 2 interface GigabitEthernet 1/1
mep 20 voe
# Enable EVC peer with MEP ID 2
mep 20 peer-mep-id 2
# Enable CCM on EVC MEP with 1 second interval
mep 20 cc 0
```

Port Protected EP-Line

The following illustration shows an EP-Line with 1:1 port protection on the NNI side. The following sections describe how the edge bridges can be configured. This setup requires more resources compared to the unprotected EP-Line, because rules must be added for both NNI ports.

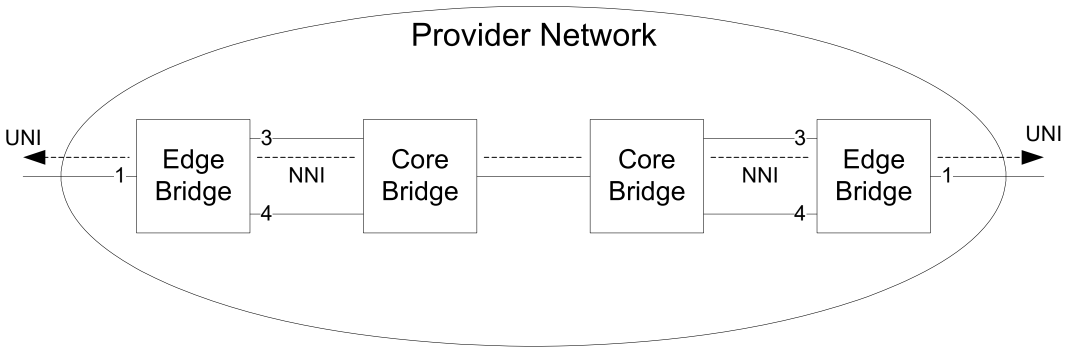


Figure 3 • **Port Protected EP-Line**

Control Protocols, VLAN, QoS, and L2CP Configuration

The following commands are used for control protocols, VLAN, and QoS configuration.

```
# Disable STP and LLDP on UNI/NNI ports
```

```
interface GigabitEthernet 1/1,3,4
 no lldp receive
 no lldp transmit
 no spanning-tree
# Exclude UNI/NNI ports from default VLAN
# Set PVID to an unused VLAN to discard non-classified frames
# UNI is C-port, NNI is S-port
interface GigabitEthernet 1/1
 switchport hybrid native vlan 4095
 switchport hybrid allowed vlan none
 switchport hybrid port-type c-port
 switchport mode hybrid
interface GigabitEthernet 1/3,4
 switchport hybrid native vlan 4095
 switchport hybrid allowed vlan none
 switchport hybrid port-type s-port
 switchport mode hybrid
# On UNI and NNI, enable ingress one-to-one mapping from PCP to CoS
interface GigabitEthernet 1/1,3,4
qos trust tag
 qos map tag-cos pcp 0 dei 0 cos 0 dpl 0
 qos map tag-cos pcp 0 dei 1 cos 0 dpl 1
 qos map tag-cos pcp 1 dei 0 cos 1 dpl 0
 qos map tag-cos pcp 1 dei 1 cos 1 dpl 1
# On UNI and NNI, enable egress one-to-one mapping from CoS to PCP
qos tag-remark mapped
 qos map cos-tag cos 0 dpl 0 pcp 0 dei 0
 qos map cos-tag cos 0 dpl 1 pcp 0 dei 1
 qos map cos-tag cos 1 dpl 0 pcp 1 dei 0
 qos map cos-tag cos 1 dpl 1 pcp 1 dei 1
# On UNI/NNI port, forward all L2CP except LLDP
interface GigabitEthernet 1/1,3,4
 evc l2cp forward 0-13,15
```

EVC Configuration

Both NNI ports are included in the EVC.

```
# Add EVC 10 using S-VID 1000 and NNI port, disable learning.
evc 10 vid 1000 ivid 1000 interface GigabitEthernet 1/3,4
```

ECE Configuration

The ECE configuration for the Advanced NNI setup is used.

```
# On UNI port, map tagged frames with PCP 4-7 to class 4, use (VID, PCP) lookup
evc ece 1 interface GigabitEthernet 1/1 outer-tag match type c-tagged pcp 4-7
add pcp-mode fixed pcp 4 tx-lookup pcp-vid evc 10 cos 4
# On UNI port, map other frames to class 0, use (VID, PCP) lookup
evc ece 2 interface GigabitEthernet 1/1 outer-tag add pcp-mode fixed pcp 0
tx-lookup pcp-vid evc 10 cos 0
```

OAM Configuration

Port MEPs are created on the NNI ports to control protection switching and L-APS is enabled on the protecting MEP.

```
# Create NNI port 3 MEP with MEG level 0 and MEP ID 3
```

```
mep 3 down domain port flow 3 level 0 interface GigabitEthernet 1/3
mep 3 meg-id ICC000MEG0000 itu
mep 3 voe
# Enable NNI peer with MEP ID 2
mep 3 peer-mep-id 2
# Enable CCM on UNI MEP with 1 second interval
mep 3 cc 0
# Create NNI port 4 MEP with MEG level 0 and MEP ID 4
mep 4 down domain port flow 4 level 0 interface GigabitEthernet 1/4
mep 4 meg-id ICC000MEG0000 itu
mep 4 voe
# Enable NNI peer with MEP ID 2
mep 4 peer-mep-id 2
# Enable CCM on NNI MEP with 1 second interval
mep 4 cc 0
# Enable L-APS transmissions
mep 4 aps 7 laps
```

EPS Configuration

An EPS instance is created based on the NNI MEPs with the APS protocol enabled.

```
# Create EPS instance using NNI ports
eps 1 domain port architecture 1for1 work-flow GigabitEthernet 1/3 protect-flow
GigabitEthernet 1/4
# Configure MEP and enable APS on EPS instance
eps 1 mep-work 3 mep-protect 4 mep-aps 4
```

Ring Protected EP-Line

The following illustration shows an EP-Line with ring protection on the NNI side. The resource consumption is similar to the port protection scenario, because rules must be added for each NNI port.

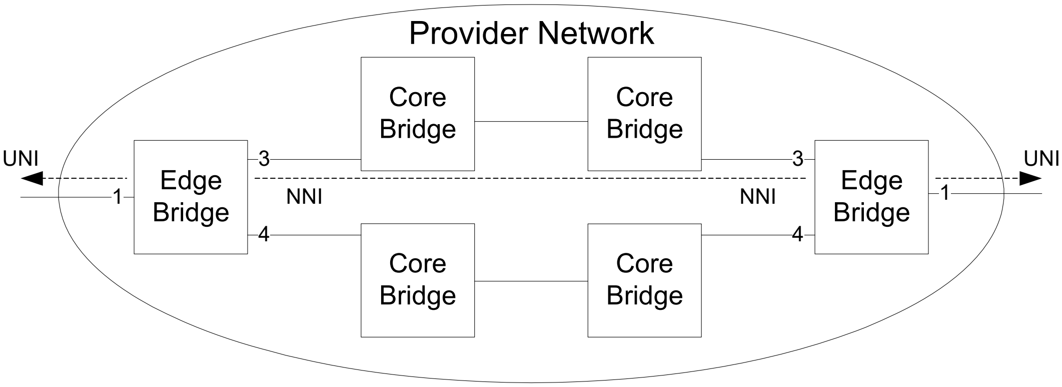


Figure 4 • **Ring Protected EP-Line**

Control Protocols, VLAN, QoS, and L2CP Configuration

The basic setup is identical to that for the "EVP-Line".

EVC Configuration

Both NNI ports are included in the EVC. ERPS requires that learning is enabled.

```
# Use quarter rules for UNI and NNI
interface GigabitEthernet 1/1,3,4
evc key double-tag
# Add EVC 10 using S-VID 1000 and NNI port, enable learning
evc 10 vid 1000 ivid 1000 interface GigabitEthernet 1/3,4 learning
```

ECE Configuration

The ECE configuration for the Advanced NNI setup is used.

```
# On UNI port, map tagged frames with PCP 4-7 to class 4, use (VID, PCP) lookup
evc ece 1 interface GigabitEthernet 1/1 outer-tag match type tagged pcp 4-7
tx-lookup pcp-vid evc 10 cos 4
# On UNI port, map other frames to class 0, use (VID, PCP) lookup
evc ece 2 interface GigabitEthernet 1/1 tx-lookup pcp-vid evc 10 cos 0
```

OAM Configuration

Port MEPs are created on the NNI ports to control protection switching using VLAN 50 and enabling R-APS on both MEPs.

```
# Create NNI port 3 MEP with MEG level 0, MEP ID 3 and vid 50
mep 3 down domain port flow 3 level 0 interface GigabitEthernet 1/3
mep 3 meg-id ICC000MEG0000 itu
mep 3 voe
mep 3 vid 50
# Enable NNI peer with MEP ID 2
mep 3 peer-mep-id 2
# Enable CCM on UNI MEP with 1 second interval
mep 3 cc 0
# Enable R-APS
mep 3 aps 7 multi raps octet 0
# Create NNI port 4 MEP with MEG level 0, MEP ID 4 and vid 50
mep 4 down domain port flow 4 level 0 interface GigabitEthernet 1/4
mep 4 meg-id ICC000MEG0000 itu
mep 4 voe
mep 4 vid 50
# Enable NNI peer with MEP ID 2
mep 4 peer-mep-id 2
# Enable CCM on UNI MEP with 1 second interval
mep 4 cc 0
# Enable R-APS
mep 4 aps 7 multi raps octet 0
```

ERPS Configuration

An ERPS instance is created based on the NNI MEPs. The EVC S-VID is enabled for this ring. The switch is setup as RPL owner on port 3. The peer switch must be RPL neighbor on this port.

```
# Create ERPS instance
erps 1 major port0 interface GigabitEthernet 1/3 port1 interface
GigabitEthernet 1/4
# Map VLAN 1000 to the ring
erps 1 vlan add 1000
```

```
# Map NNI MEPs to ring
erps 1 mep port0 sf 3 aps 3 port1 sf 4 aps 4
# Set as RPL owner on port 3
erps 1 rpl owner port0
```

EVP-Line

Unprotected EVP-Line

The following illustration shows an unprotected EVP-Line forwarding frames with C-VID 17 between the UNI ports.

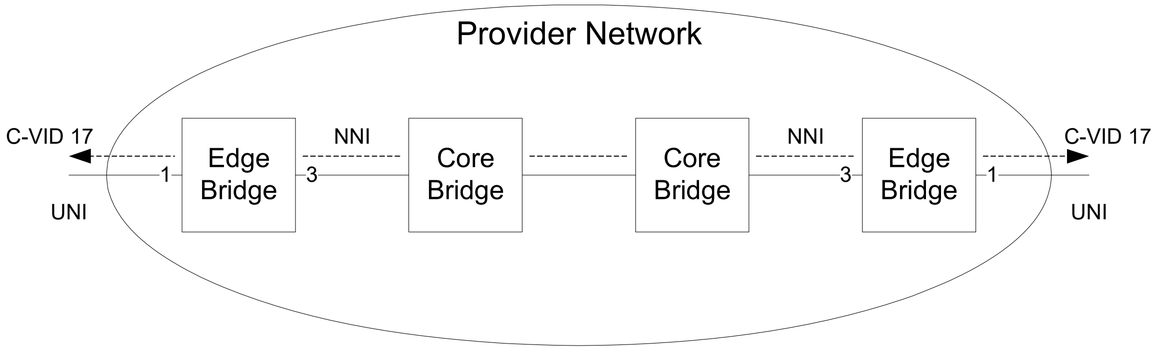


Figure 5 • **Unprotected EVP-Line**

Control Protocols, VLAN, and QoS Configuration

The setups are identical to those for the "EP-Line".

L2CP Configuration

All L2 control protocols except LLDP must be tunneled over the EVC. LLDP uses DMAC 01-80-C2-00-00-0E corresponding to L2CP ID 14. ACL policy 42 is used to identify an L2CP profile because multiple EVP-Lines may be set up on the UNI port with different L2CP forwarding properties, and, as a result, the configuration cannot be based on the port alone. An ACL rule matching this policy and the UNI port is set up to discard LLDP frames.

```
# On UNI/NNI port, forward all L2CP.
interface GigabitEthernet 1/1,3
 evc l2cp forward 0-13,15
# Discard LLDP frames using ACL rule matching policy 42
access-list ace 1 policy 0x2a policy-bitmask 0x3F tag-priority 0 frametype
etype dmac 01-80-c2-00-00-0e action deny
```

EVC Configuration

The EVC setup is identical to that for the "EP-Line".

ECE Configuration

The ECEs are added using the advanced NNI method. Two service classes are used based the PCP. Only tagged frames with C-VID 17 are mapped to the EVC. The ECEs are mapped to ACL policy 42 for L2CP frame handling.

```
# On UNI port, map tagged frames with PCP 4-7 to class 4, use (VID, PCP) lookup
evc ece 1 interface GigabitEthernet 1/1 outer-tag match type c-tagged vid 17
pcp 4-7 add pcp-mode fixed pcp 4 tx-lookup pcp-vid evc 10 cos 4 policy 42
# On UNI port, map other frames to class 0, use (VID, PCP) lookup
evc ece 2 interface GigabitEthernet 1/1 outer tag match type c-tagged vid 17
add pcp-mode fixed pcp 0 tx-lookup pcp-vid evc 10 cos 0 policy 42
```

OAM Configuration

OAM MEP setup is identical to that for the "EP-Line".

E-Tree

Ethernet services have been increasingly deployed by carriers over the last few years through E-Line (point-to-point) services and E-LAN (multipoint-to-multipoint) services. In a variety of scenarios, an enterprise needs to distribute data from one or multiple sources (or roots) to a large number of destinations (or leaves). These scenarios might include multimedia companies distributing video streams to affiliated stations, financial institutions distributing market data to their clients, and organizations utilizing live video remote training or presentations.

The main requirements of such designs are:

- Almost uni-directionality of the data stream (for instance, from the root to the leaves)
- A relatively limited amount of data from the leaves back to the root
- Lack of communication between the leaves

It is a new type of Ethernet service over infrastructure. E-Trees classify root UNIs and leaf UNIs. Data can be exchanged root-to-root or root-to-leaf, but not leaf-to-leaf. Services over E-Tree are compatible with the wide range of Ethernet products offered by carriers today. They also have the proven potential to support new possibilities and applications such as video distribution, mobile backhaul, and clock synchronization.

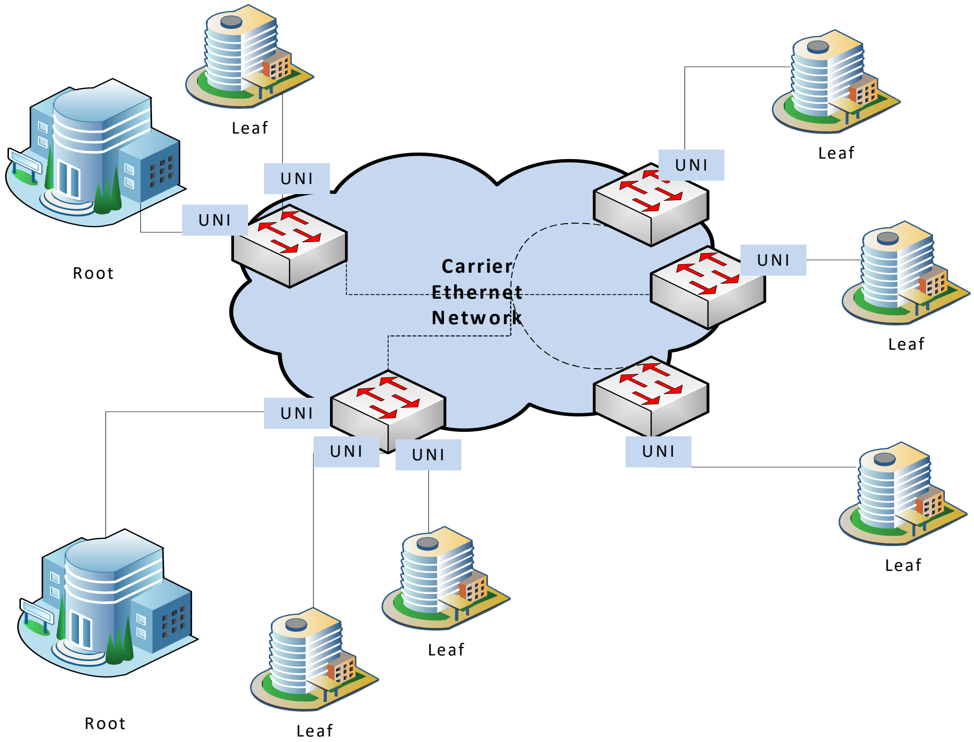


Figure 6 • **E-Tree Diagram**

Advantages of E-Tree

- The advantages of E-tree include:
- Improved video broadcasting
- Network infrastructure sharing
- Bandwidth optimization
- Reduced network infrastructure cost

Platform Support

E-tree is supported on Cisco ME1200.

E-Tree Use Model

MEF defines an E-Tree as a Rooted-Multipoint EVC based on two UNI types:

- Leaf UNI

- Root UNI

Frames from leaf UNIs may only be delivered to root UNIs. Frames from root UNIs may be delivered to leaf and root UNIs. The following illustration shows an E-Tree implemented using two VLANs with shared VLAN learning as recommended by IEEE802.1Q-2011, Annex F.1.3.

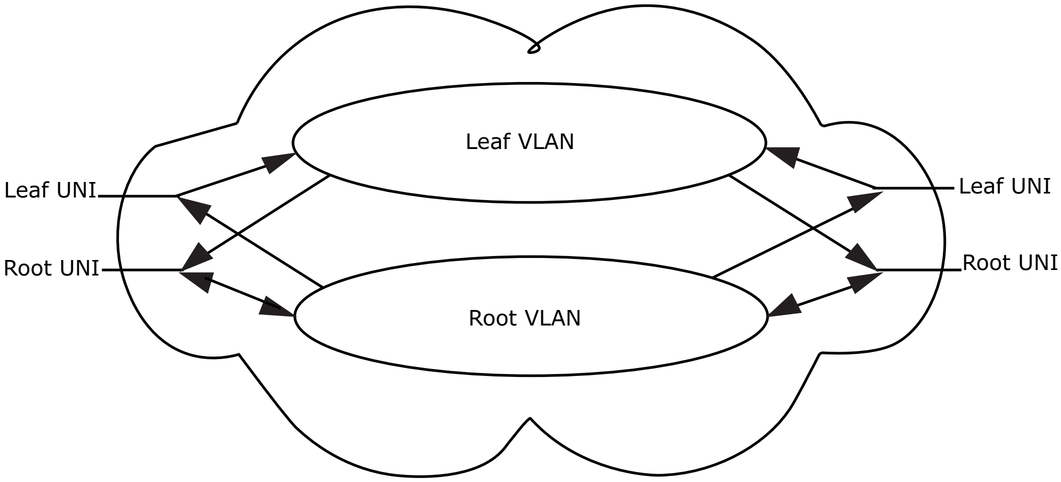


Figure 7 • **E-Tree Use Model**

The leaf VLAN receives frames from leaf ports and sends frames to root ports only. The root VLAN receives frames from root ports and sends frames to leaf and root ports.

Configuring E-Tree

This section describes how to configure an E-Tree that enables additional connectivity choices for enterprises

Configuring E-Tree using the CLI

The following example shows how to configure E-Tree from the CLI. This service has two UNIs (one leaf UNI and one root UNI) and one NNI port. In this example, both the leaf and the root are on the same switch.

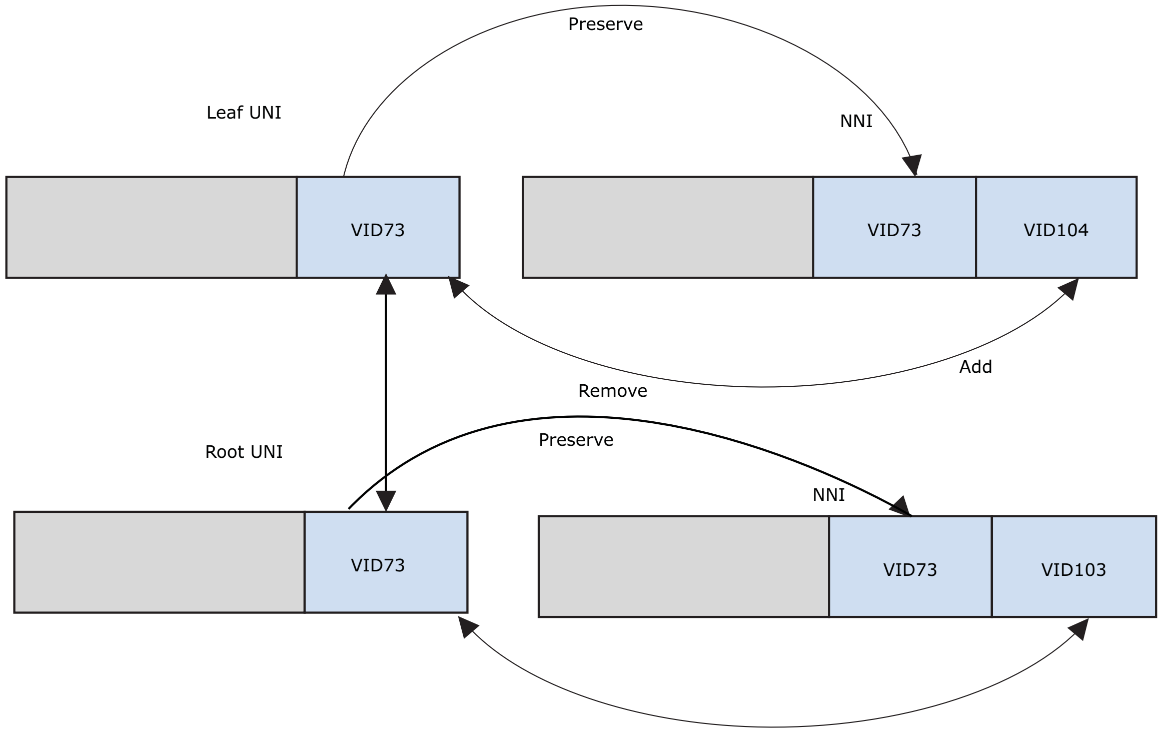


Figure 8 **• Example of E-Tree**

1. Set up an E-tree service (no-bundling) on a leaf UNI (Port 2) for CEVLAN ID 73
2. Set up an E-tree service (no-bundling) on a root UNI (Port 3) for CEVLAN ID 73
3. On NNI egress, add one tag: outer VID=103 (root), VID = 104 (Leaf)
4. On NNI ingress, pop one tag
5. Match on a NNI (port 4) for Root VID=103 or Leaf VID = 104 and inner VID=73

Configuration:

1. Map VLAN 104 and 103 to FID 10

```
svl fid 10 vlan 104,103
```

2. Create an EVC as described above.

```
evc 6 vid 103 ivid 103 interface GigabitEthernet 1/1 leaf vid 104 ivid 104 
interface
GigabitEthernet 1/2 learning policer none
```

Where,

```
evc-id = 6
NNI vid = 103
NNI ivid = 103
NNI port-id = 1/1 leaf vid = 104 leaf ivid = 104
Leaf port-id = 1/2
```

3. Create an ECE for UNI#1 (Leaf UNI).

```
evc ece 1 interface GigabitEthernet 1/2 outer-tag match type tagged vid 73 evc
6 policer none
```

Where,

```
ece-id = 1 port-id = 1/2 vid = 73
evc-id = 6
```

4. Create an ECE for UNI#2 (Root UNI).

```
evc ece 2 interface GigabitEthernet 1/3 outer-tag match type tagged vid 73 evc
6 policer none
```

Where,

```
ece-id = 2 port-id = 1/3 vid = 73
evc-id = 6
```

Table 1 • **Control Field Details**

Field	Description
UNI Ports	
UNI Ports	The list of User Network Interfaces for the ECE.
Ingress Matching	
Lookup	The lookup type for matching the ECE. The allowed values are: `Basic:` First lookup for basic classification. `Advanced:` Second lookup for advanced classification.
Tag Type	The tag type for matching the ECE. The possible values are: Any: The ECE matches with both tagged and untagged frames. Untagged: The ECE matches with the untagged frames only. C-Tagged: The ECE matches with the custom tagged frames only. S-Tagged: The ECE matches with the service tagged frames only. Tagged: The ECE matches with the tagged frames only.
Inner Tag Type	The inner tag type for matching the ECE. The possible values are: Any: The ECE matches with both tagged and untagged frames. Untagged: The ECE matches with the untagged frames only. Tagged: The ECE matches with the tagged frames only.
Frame Type	The frame type for the ECE. The possible values are: Any: The ECE matches with any frame type. IPv4: The ECE matches with the IPv4 frames only. IPv6: The ECE matches with the IPv6 frames only. Ethernet Type: The ECE matches with the Ethernet type frames only. LLC: The ECE matches with the LLC frames only. SNAP: The ECE matches with the SNAP frames only. L2CP: The ECE matches with the L2CP frames only.
Actions	
Directions	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, then the ingress rules of the NNI ports is setup to match the traffic being forwarded to NNI ports. The possible values are: `Both:` Bidirectional. `UNI-to-NNI:` Unidirectional from UNI to NNI. `NNI-to-UNI:` Unidirectional from NNI to UNI.
Rule Type	The TX lookup for the ECE. The possible values are: `VID lookup` : The TX lookup is based on VID. VID-PCP: The TX lookup is based on VID and PCP. ISDX : The TX lookup is based on ISDX.

Table 1 • **Control Field Details (continued)**

Field	Description
TXL Lookup	Attach EVC to the MPLS Pseudo-Wires.
L2CP Mode	The L2CP mode for the ECE. The possible values are: Forward: Forward with unchanged DMAC. Tunnel: Forward EType/LLC/SNAP frame and replace DMAC. Discard: Drop frame. Peer: Process frame by local protocol entity.
L2CP DMAC	The L2CP destination MAC for the ECE. The possible values are: Custom: The L2CP destination MAC address is based on IEEE L2CP MAC addresses (01-00-0C-CD-CD-0X or 01-00-0C-CD-CD-2X). Cisco: The L2CP destination MAC address is based on Cisco L2CP MAC address (01-00-0C-CD-CD-D0).
EVC ID Filter	The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. The possible values are: Any: No EVC ID filter is specified. (EVC ID filter status is "don't-care".) Specific: If you want to filter a specific EVC ID with this ECE, choose this value. A field for entering a specific value appears.
EVC ID Value	When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is from 1 through 1024 .
Policer ID Filter	The policer ID filter for matching the ECE. The possible values are: Specific: If you want to filter a specific policer ID value with this ECE, then choose this value. A field for entering a specific value appears. Discard: All received frames are discarded for the ECE. None : All received frames are forwarded for the ECE. None: The bandwidth profile for the specified EVC ID is used.
Policer ID Value	When "Specific" is selected for the policer ID filter, you can enter a specific value. The value is from 1 through 1022.
Tag Pop Count	The ingress tag pop count for the ECE. The allowed range is from 0 through 2.
Policy ID	The ACL Policy ID for the ECE for matching ACL rules. The allowed range is from 0 through 63.
Class	The traffic class for the ECE. The allowed range is from 0 through 7 or disabled.
Drop Precedence	The drop precedence for the ECE. The allowed range is 0 , 1 or disabled.
MAC Parameters	
SMAC Filter	The source MAC address for matching the ECE. The possible values are: Any: No SMAC filter is specified. (SMAC filter status is "don't-care".) Specific: If you want to filter a specific SMAC value with this ECE, then choose this value. A field for entering a specific value appears.
DMAC Filter	When "Specific" is selected for the SMAC filter, you can enter a specific value. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit).
Egress Outer Tag/Egress Inner Tag	
Egress 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.

Table 1 • **Control Field Details (continued)**

Field	Description
Ingress Type	The inner type for the ECE determines whether an inner tag is inserted in frames forwarded to NNI ports. The possible values are: None: An inner tag is not inserted. C-tag: An inner C-tag is inserted. S-tag: An inner S-tag is inserted. S-custom-tag: An inner tag is inserted and the tag type is determined by the VLAN port configuration of the NNI.
VLAN ID	The EVC outer/inner tag VID for UNI ports. The allowed value is from 1 through 4095.
PCP Mode	The outer/inner tag PCP value for the ECE. The allowed range is from 0 through 7.
PCP	The outer/inner tag PCP value for the ECE. The allowed range is from 0 through 7.
DEI Mode	The outer/inner tag DEI mode for the ECE. The possible values are: Classified: The outer tag DEI mode is classified. Fixed : The outer tag DEI mode is fixed. Drop Precedence: The outer tag DEI mode is drop precedence.
DEI	The outer/inner tag DEI value for the ECE. The allowed value is 0 or 1.

EP-Tree

Unprotected EP-Tree

The following illustration shows a Provider Network offering an unprotected Ethernet Private Tree between two Leaf UNIs and two root UNIs. Two VLANs are used to form the E-Tree.

- The root VLAN is used for frames received on root UNIs.
- The leaf VLAN is used for frames received on leaf UNIs.

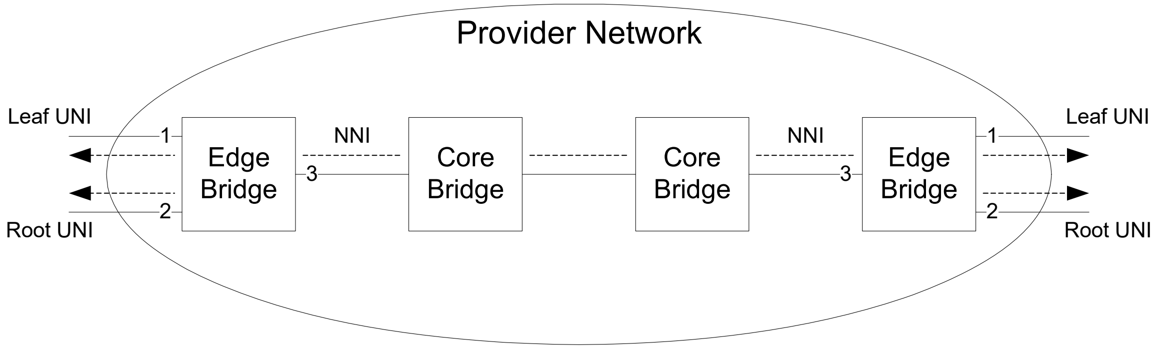


Figure 9 • **Unprotected EP-Tree**

Control Protocols, VLAN, and QoS Configuration

The following commands are executed to disable control protocols and setup VLAN and QoS for the UNI and NNI ports. Shared VLAN learning is enabled for VLAN 10 and 20, which will be used as root and leaf VLAN.

```
# SVL: Map VLAN 10 and 20 to FID 10
svl fid 10 vlan 10,20
# Disable STP and LLDP on UNI/NNI ports
interface GigabitEthernet 1/1-3
 no lldp receive
 no lldp transmit
 no spanning-tree
# Exclude UNI/NNI ports from all VLANs
# Set PVID to an unused VLAN to discard non-classified frames
# UNIs are C-port, NNI is S-port
interface GigabitEthernet 1/1-2
 switchport hybrid native vlan 4095
 switchport hybrid allowed vlan none
 switchport hybrid port-type c-port
 switchport mode hybrid
interface GigabitEthernet 1/3
 switchport hybrid native vlan 4095
 switchport hybrid allowed vlan none
 switchport hybrid port-type s-port
 switchport mode hybrid
# Enable ingress one-to-one mapping from PCP to CoS
interface GigabitEthernet 1/1-3
 qos trust tag
 qos map tag-cos pcp 0 dei 0 cos 0 dpl 0
 qos map tag-cos pcp 0 dei 1 cos 0 dpl 1
 qos map tag-cos pcp 1 dei 0 cos 1 dpl 0
 qos map tag-cos pcp 1 dei 1 cos 1 dpl 1
# Enable egress one-to-one mapping from CoS to PCP
 qos tag-remark mapped
 qos map cos-tag cos 0 dpl 0 pcp 0 dei 0
 qos map cos-tag cos 0 dpl 1 pcp 0 dei 1
 qos map cos-tag cos 1 dpl 0 pcp 1 dei 0
 qos map cos-tag cos 1 dpl 1 pcp 1 dei 1
```

EVC Configuration

The EVC is set up with the leaf and root VLANs and leaf UNI list.

```
# Add EVC 10 using Root VID 10 and Leaf VID 20
evc 10 vid 10 ivid 10 interface GigabitEthernet 1/3 leaf vid 20 ivid 20
interface GigabitEthernet 1/1 learning
```

ECE Configuration

The ECE configuration for the advanced NNI setup is used.

```
# Map tagged frames with PCP 4-7 to class 4, use (VID, PCP) lookup
evc ece 1 interface GigabitEthernet 1/1-2 outer-tag match type c-tagged pcp
4-7 add pcp-mode fixed pcp 4 tx-lookup pcp-vid evc 10 cos 4
# Map other frames to class 0, use (VID, PCP) lookup
evc ece 2 interface GigabitEthernet 1/1-2 outer-tag add pcp-mode fixed pcp 0
tx-lookup pcp-vid evc 10 cos 0
```

L2CP Processing

The previous sections describe how L2CP frames can be discarded using EVC port configuration (EP-Line) or ACL rules (EVP-Line). This section describes more advanced L2CP processing, again using LLDP as the example. The EVC configurations described in the previous sections can be reused, if the L2CP configuration parts are replaced by the L2CP configuration shown in the following sections.

Peering

Peering is done by default for LLDP, as a result, the following commands are only needed if the LLDP or L2CP configuration for the UNI has been changed.

```
# Enable and Peer LLDP
interface GigabitEthernet 1/1
 lldp receive
 lldp transmit
 evc update l2cp peer 14
```

Discarding

Discarding LLDP at a UNI is done using the L2CP mode for the port.

```
# Discard L2CP
interface GigabitEthernet 1/1
 evc update l2cp discard 14
```

Forwarding

Forwarding LLDP over an EVC requires that the UNI and NNI are set up to forward the protocol. LLDP frames will then be treated like other frames forwarded over the EVC.

```
# Forward LLDP
interface GigabitEthernet 1/1,3
 evc update l2cp forward 14
```

Tunneling

L2CP tunneling means that the DMAC of the L2CP frame is replaced by a tunnel DMAC when forwarding from UNI to NNI port. When forwarding from NNI to UNI port, the tunnel DMAC is replaced with the original L2CP DMAC. This can be used to avoid core bridges inside the provider network processing the frames as L2CP frames.

L2CP tunneling requires that the advanced ingress lookup is used for classification on UNI ports. It also requires that the EVC is set up with a specific ACL policy. The ECE configuration for the Advanced NNI setup is used in the following example, using ACL policy 42. For more information, see "Advanced NNI" on page 5.

```
# Map tagged frames with PCP 4-7 to class 4, use (VID, PCP) lookup
evc ece 1 interface GigabitEthernet 1/1 outer-tag match type c-tagged pcp 4-7 add pcp-mode
fixed pcp 4 tx-lookup pcp-vid evc 10 cos 4 policy
42
# Map other frames to class 0, use (VID, PCP) lookup
evc ece 2 interface GigabitEthernet 1/1 outer-tag add pcp-mode fixed pcp 0 tx-lookup
pcp-vid evc 10 cos 0 policy 42
# Tunnel LLDP frames
```

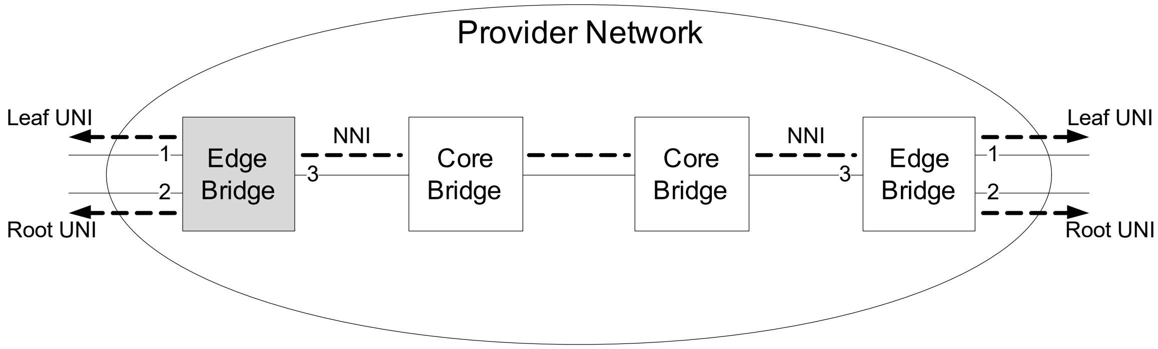
```
evc ece 3 lookup advanced interface GigabitEthernet 1/1 frame-type l2cp lldp outer-tag
add pcp-mode fixed pcp 4 tx-lookup pcp-vid evc 10 cos 4 policy 42 l2cp mode tunnel
# Forward LLDP frames and use half key advanced ingress lookup
interface GigabitEthernet 1/1
evc update key-advanced normal l2cp forward 14
```

Ethernet Private Tree (EP-Tree)

The diagram below shows a provider network offering an EP- Tree between two Leaf UNIs and two Root UNIs. Two VLANs are used to form the E-Tree:

- The Root VLAN is used for frames received on Root UNIs.
- The Leaf VLAN is used for frames received on Leaf UNIs.

Figure 10 • **EP-Tree**



In the example, the Root VLAN uses S-VID 1000 and the Leaf VLAN uses S-VID 1001. Shared VLAN Learning is setup for the two VLANs.

Configuration Summary

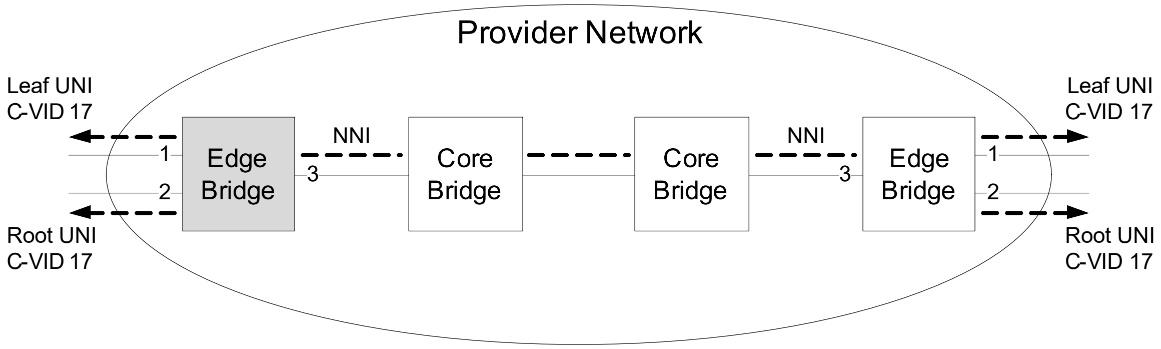
The following code block shows the relevant parts of the running configuration.

```
evc 10 vid 1000 ivid 1000 leaf vid 1001 ivid 1001 learning nni ingress-map 20 egress-map 30
evc ece 2 interface GigabitEthernet 1/1-2 outer-tag match type untagged frame-type l2cp cdp evc 10
l2cp mode tunnel
evc ece 1 interface GigabitEthernet 1/1-2 evc 10 ingress-map 20
evc encapsulation 5 vid 2000 egress-map 30
svl fid 1000 vlan 1001
!
qos map ingress 20
 action class
 map pcp 4 dei 0 to class 1
 map pcp 5 dei 0 to class 1
 map pcp 6 dei 0 to class 1
 map pcp 7 dei 0 to class 1
!
qos map egress 30
 action pcp
 map class 1 dpl 0 to pcp 4
!
interface GigabitEthernet 1/1
 switchport hybrid native vlan 4095
 switchport hybrid allowed vlan none
 switchport mode hybrid
 no lldp receive
 no lldp transmit
 no spanning-tree
 evc l2cp forward 14 discard 0-13,15
 evc rule 10 role leaf encapsulation disable l2cp disable
 evc policer 10 class 0 enable rate-type line cir 1000 eir 1000
 evc policer 10 class 1 enable rate-type line cir 2000 eir 2000
 evc l2cp 14 class 1
!
interface GigabitEthernet 1/2
 switchport hybrid native vlan 4095
 switchport hybrid allowed vlan none
 switchport mode hybrid
 no lldp receive
 no lldp transmit
 no spanning-tree
 evc l2cp forward 14 discard 0-13,15
 evc rule 10 role root encapsulation disable l2cp disable
 evc policer 10 class 0 enable rate-type line cir 1000 eir 1000
 evc policer 10 class 1 enable rate-type line cir 2000 eir 2000
 evc l2cp 14 class 1
!
interface GigabitEthernet 1/3
 switchport hybrid native vlan 4095
 switchport hybrid allowed vlan none
 switchport hybrid port-type s-port
 switchport mode hybrid
 no lldp receive
 no lldp transmit
 no spanning-tree
 evc rule 10 role nni encapsulation 5 l2cp disable
!
```

Ethernet Virtual Private Tree (EVP-Tree)

The diagram below shows a provider network offering an EVP-Tree forwarding frames with C-VID 17 between the UNI ports.

Figure 11 **• EVP-Tree**



Configuration Summary

The following code block shows the relevant parts of the running configuration.

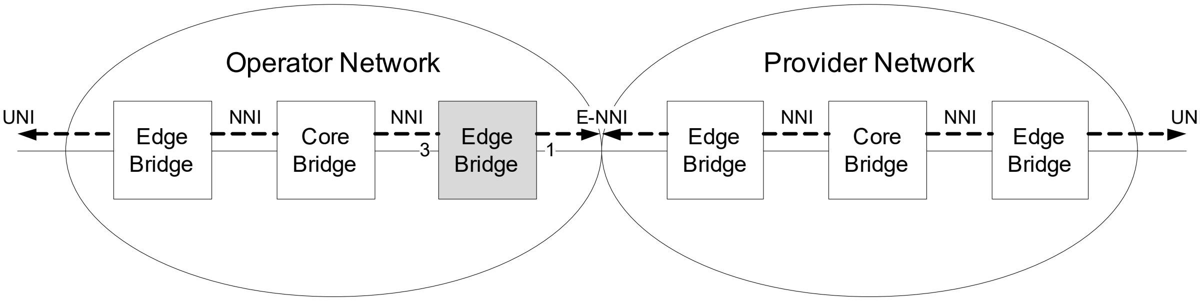
```
evc 10 vid 1000 ivid 1000 leaf vid 1001 ivid 1001 learning nni ingress-map 20 egress-map 30
evc ece 2 interface GigabitEthernet 1/1-2 outer-tag match type c-tagged vid 17 frame-type l2cp cdp
evc 10 l2cp mode tunnel ingress-map 20
evc ece 1 interface GigabitEthernet 1/1-2 outer-tag match type c-tagged vid 17 evc 10 ingress-map
20
evc encapsulation 5 vid 2000 egress-map 30
evc l2cp 6 14 forward class 1
svl fid 1000 vlan 1001
!
qos map ingress 20
 action class
 map pcp 4 dei 0 to class 1
 map pcp 5 dei 0 to class 1
 map pcp 6 dei 0 to class 1
 map pcp 7 dei 0 to class 1
!
qos map egress 30
 action pcp
 map class 1 dpl 0 to pcp 4
!
interface GigabitEthernet 1/1
 switchport hybrid native vlan 4095
 switchport hybrid allowed vlan none
 switchport mode hybrid
 no lldp receive
 no lldp transmit
 no spanning-tree
 evc rule 10 role leaf encapsulation disable l2cp 6
 evc policer 10 class 0 enable rate-type line cir 1000 eir 1000
 evc policer 10 class 1 enable rate-type line cir 2000 eir 2000
!
interface GigabitEthernet 1/2
 switchport hybrid native vlan 4095
 switchport hybrid allowed vlan none
 switchport mode hybrid
 no lldp receive
 no lldp transmit
 no spanning-tree
 evc rule 10 role root encapsulation disable l2cp 6
 evc policer 10 class 0 enable rate-type line cir 1000 eir 1000
 evc policer 10 class 1 enable rate-type line cir 2000 eir 2000
!
interface GigabitEthernet 1/3
 switchport hybrid native vlan 4095
 switchport hybrid allowed vlan none
 switchport hybrid port-type s-port
 switchport mode hybrid
 no lldp receive
 no lldp transmit
 no spanning-tree
 evc rule 10 role nni encapsulation 5 l2cp 0
!
```

E-Access

The following illustration shows a service provider offering an EVC based on an E-Access OVC provided by an access operator. The focus is one the right Edge Bridge in the Operator Network. At the E-NNI, the OVC is identified by a single S-VID. Inside the Operator Network, another S-VID is used to transport the OVC, and all frames are mapped into a single CoS.

The EVC provided from UNI to UNI could be an EP-Line or EVP-Line.

Figure 12 • **E-Access**



Configuration Summary

The E-Access configuration example is shown below. The E-NNI is an S-port with the same EVC role as a UNI (‘root’). The NNI port is also an S-port. The ECE rule matches and pops S-VID 1000 on the E-NNI. An encapsulation entry is used to add S-VID 100 when forwarding to the E-NNI.

Frames received on the E-NNI are processed by a MEF policer for COSID 0.

```
evc 10 vid 100 ivid 100
evc ece 1 interface GigabitEthernet 1/1 outer-tag match type s-tagged vid 1000 evc 10 pop 1
evc encapsulation 5 vid 1000 egress-map 0
interface GigabitEthernet 1/1
 switchport hybrid native vlan 4095
 switchport hybrid allowed vlan none
 switchport hybrid port-type s-port
 switchport mode hybrid
 no lldp receive
 no lldp transmit
 no spanning-tree
 evc rule 10 role root encapsulation 5 l2cp disable
 evc policer 10 class 0 enable rate-type line cir 1000 eir 1000
!
interface GigabitEthernet 1/3
 switchport hybrid native vlan 4095
 switchport hybrid allowed vlan none
 switchport hybrid port-type s-port
 switchport mode hybrid
 no lldp receive
 no lldp transmit
 no spanning-tree
 evc rule 10 role nni encapsulation disable l2cp disable
```

CHAPTER 6

MEF Services Configuration

This document describes how to configure MEF E-Line and E-LAN services on Cisco ME1200.

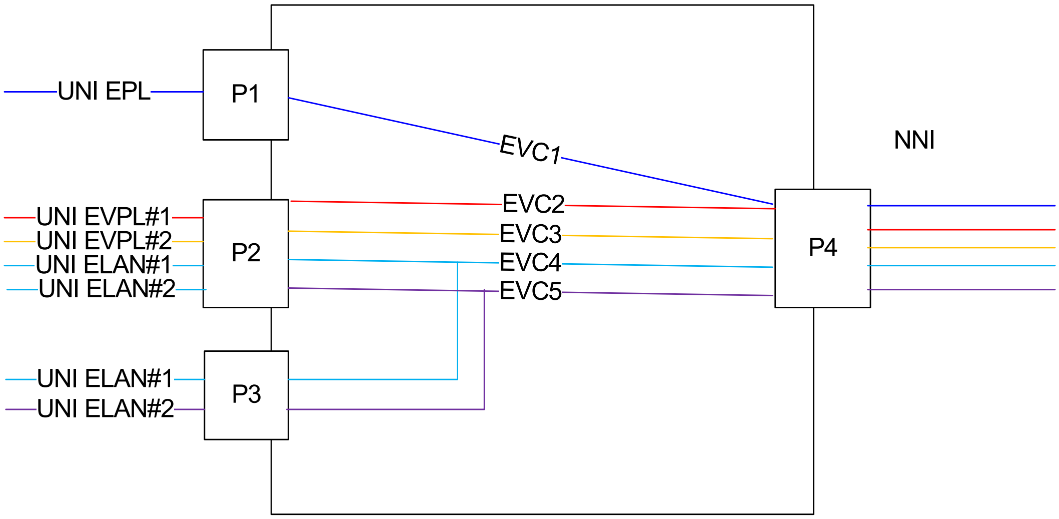


Figure 1 • **Service Configuration Overview**

EPL Service between UNI and NNI

This section lists the steps to set up a service with the following attributes.

1. EPL service (all to one bundling) on a UNI (port 1)
2. Add a tag (54) on NNI (port 4)

3. Pop/remove the tag on UNI egress

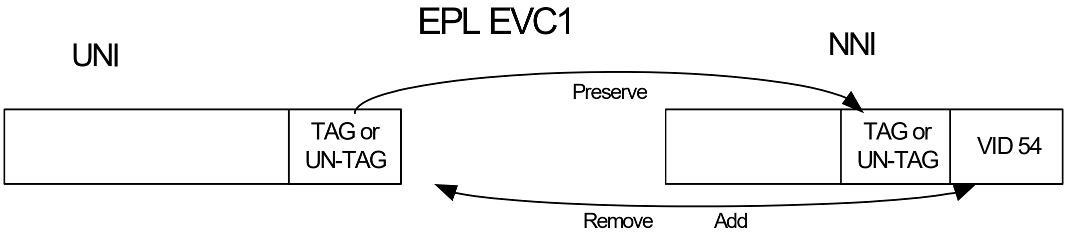


Figure 2 • **EPL EVC1 FLow**

Create EVC

The following configuration settings are used to create the EVC.

- VID = 54.
- IVID = 54 (internal VID used for internal classification, which may use any unique value).
- Learning is disabled because this is a point-to-point service.
- NNI port 4 is used.
- No inner tag is specified because double VLAN tagging on the NNI is not used.
- The outer tag VID is not specified because it is used for uni-directional NNI to UNI service.

EVC ICLI Command

```
# evc 1 vid 54 ivid 54 interface GigabitEthernet 1/4 policer none
```

Create EVC Control Entry (ECE)

The following service parameters and actions are used to create the ECE, which controls the UNI configuration.

Service Parameters

- UNI port =1.
- UNI matching is any for all to one bundling. MAC parameters are set to any.
- NNI outer tag is not specified because it is used to insert a tag on the UNI for uni-directional services.

Actions

- EVC ID = 1.
- Direction = Both (bi-directional service).
- Tag Pop Count = 0 for EPL service (all frames are passed to the EVC without popping any tags).
- Policy ID = 0 because this service is not using any policer. The policy ID is used to point to an ACL so that the ACL can then be used to select an EVC policer.

ECE ICLI Command

```
# evc ece 1 interface GigabitEthernet 1/1 policer none
```

EVPL Service between UNI and NNI (Bundle 1)

This section lists the steps to set up a service with the following attributes.

1. EVPL service (bundling) on a UNI (port 2) for CEVLAN IDs 10-20
2. Add a tag (54) on NNI (port 4)
3. Pop/remove the tag on UNI egress

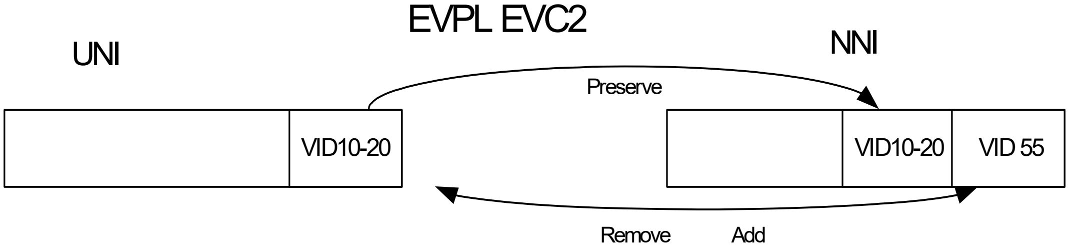


Figure 3 • **EVPL EVC2 FLow**

Create EVC

The following configuration settings are used to create the EVC.

- VID = 55.
- IVID = 55 (internal VID used for internal classification, which may use any unique value).
- Learning is disabled because this is a point-to-point service.
- NNI port 4 is used.

EVC ICLI Command

```
# evc 2 vid 55 ivid 55 interface GigabitEthernet 1/4 policer none
```

Create EVC Control Entry (ECE)

The following service parameters and actions are used to create the ECE.

Service Parameters

- UNI port = 2.
- UNI matching VID 10-20.
- MAC parameters are set to any.
- NNI outer tag is allowed to insert a tag on the UNI. This is for uni-directional services only, and it is not used in this case.

Actions

- EVC ID = 2.
- Direction = Both (bi-directional service).
- Tag Pop Count = 0 for EVPL service (all frames are passed to the EVC without popping any tags; UNI tag is preserved).

- Policy ID = 0 because this service is not using any policer. The policy ID is used to point to an ACL so that the ACL can then be used to select an EVC policer.

ECE ICLI Command

```
# evc ece 1 interface GigabitEthernet 1/2 outer-tag match type tagged vid 10-20
evc 2 policer none
```

EVPL Service between UNI and NNI (Bundle 2)

This section lists the steps to set up a service with the following attributes.

1. EVPL service (bundling) on a UNI (port 2) for CEVLAN IDs 61, 63, 65
2. Add a tag (56) on NNI (port 4)
3. Pop/remove the tag on UNI egress

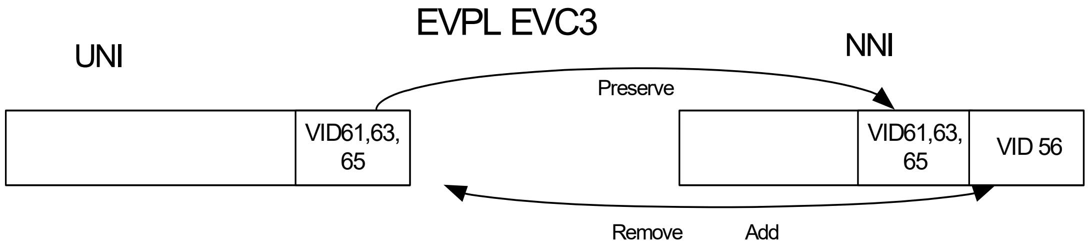


Figure 4 • **EVPL EVC3 Flow**

The following configuration settings are used to create the EVC.

- VID = 56.
- IVID = 56 (internal VID used for internal classification, which may use any unique value).
- Learning is disabled because this is a point-to-point service.
- NNI port 4 is used.

EVC ICLI Command

```
# evc 3 vid 56 ivid 56 interface GigabitEthernet 1/4 policer none
```

Create EVC Control Entry (ECE)

The following service parameters and actions are used to create the ECE.

Service Parameters

- UNI port = 2.
- UNI matching VID = 61.
- MAC parameters are set to any.
- NNI outer tag is allowed to insert a tag on the UNI. This is for uni-directional services only, and it is not used in this case.

Actions

- EVC ID = 3.
- Direction = Both (bi-directional service).
- Tag Pop Count = 0 for EVPL service (all frames are passed to the EVC without popping any tags; UNI tag is preserved).
- Policy ID = 0 because this service is not using any policer. The policy ID is used to point to an ACL so that the ACL can then be used to select an EVC policer.

ECE ICLI Command

```
# evc ece 2 interface GigabitEthernet 1/2 outer-tag match type tagged vid 61
evc 3 policer none
# evc ece 3 interface GigabitEthernet 1/2 outer-tag match type tagged vid 63
evc 3 policer none
# evc ece 4 interface GigabitEthernet 1/2 outer-tag match type tagged
vid 65 evc 3 policer none
```

LAN Service between Two UNIs and One NNI

This section lists the steps to set up three ports with the following attributes.

1. ELAN service (no-bundling) on a UNI (port 2) for CEVLAN ID 70
2. On UNI (port 2) egress swap tag with 70
3. ELAN service (bundling) on a UNI (port 3) for CEVLAN ID 80
4. On UNI (port 3) egress swap tag with 80
5. Add tag 57 on NNI egress
6. Pop tag on NNI ingress
7. Match on NNI (port 4) for VID 57

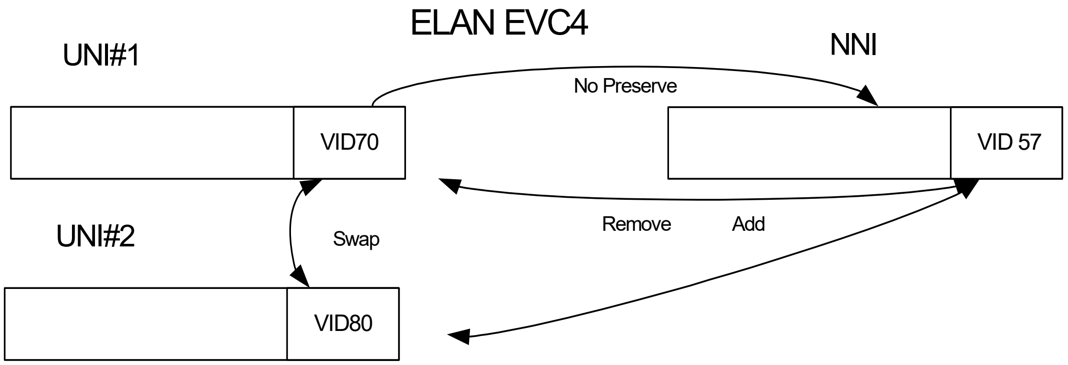


Figure 5 • **ELAN EVC4 Flow**

Create EVC

The following configuration settings are used to create the EVC.

- VID = 57.
- IVID = 57 (internal VID used for internal classification, which may use any unique value).
- Learning is enabled because this is a LAN service.

- NNI port 4 is used.

EVC ICLI Command

```
# evc 4 vid 57 ivid 57 interface GigabitEthernet 1/4 policer none
```

Create EVC Control Entry (ECE) for UNI 1

The following service parameters and actions are used to create the ECE for UNI 1.

Service Parameters

- UNI port = 2.
- UNI matching VID = 70.
- MAC parameters are set to any.
- NNI outer tag is allowed to insert a tag on the UNI. This is for uni-directional services only, and it is not used in this case.

Actions

- EVC ID = 4.
- Direction = Both (bi-directional service).
- Tag Pop Count = 1 for ELAN service (all frames are passed to the EVC popping one tag in the direction UNI to NNI and pushing one tag the other direction).
- Policy ID = 0 because this service is not using any policer. The policy ID is used to point to an ACL so that the ACL can then be used to select an EVC policer.

ECE ICLI Command

```
# evc ece 1 next last interface GigabitEthernet 1/2 outer-tag match type tagged
vid 70 evc 4 policer none pop 1
```

Create EVC Control Entry (ECE) for UNI 2

The following service parameters and actions are used to create the ECE for UNI 2.

Service Parameters

- UNI port = 3.
- UNI matching VID = 80.
- MAC parameters are set to any.
- NNI outer tag is allowed to insert a tag on the UNI. This is for uni-directional services only, and it is not used in this case.

Actions

- EVC ID = 4.
- Direction = Both (bi-directional service).

- Tag Pop Count = 1 for ELAN service (all frames are passed to the EVC popping one tag in the direction UNI to NNI and pushing one tag the other direction).
- Policy ID = 0 because this service is not using any policer. The policy ID is used to point to an ACL so that the ACL can then be used to select an EVC policer.

ECE ICLI Command

```
# evc ece 2 next last interface GigabitEthernet 1/3 outer-tag match type tagged
vid 80 evc 4 policer none pop
```

ELAN Service between Two UNIs and One NNI (DoubleTag)

This section lists the steps to set up three ports with the following attributes.

1. ELAN service (no-bundling) on a UNI (port 2) for CEVLAN ID 71
2. On UNI (port 2) egress swap tag with 71
3. ELAN service (bundling) on a UNI (port 3) for CEVLAN ID 81
4. On UNI (port 3) egress swap tag with 81
5. Add outer VID = 101 and inner VID = 58 on NNI egress
6. Pop two tags on NNI ingress
7. Match on NNI (port 4) for outer VID = 101 and inner VID = 58

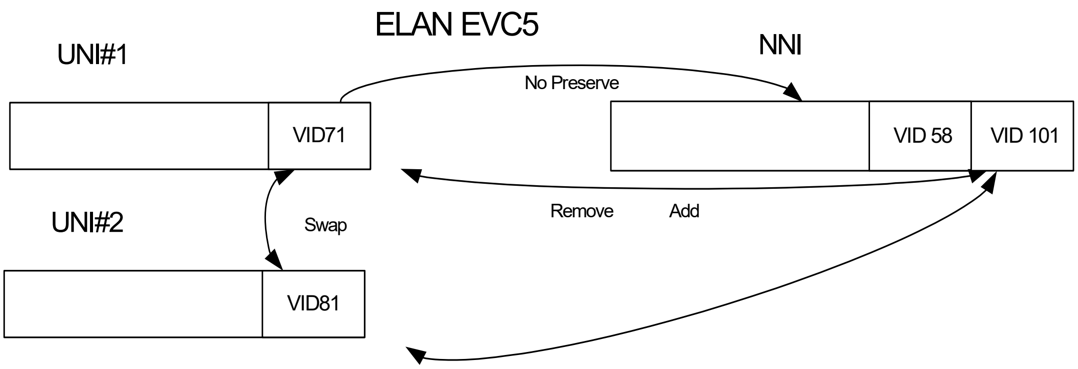


Figure 6 **• ELAN EVC5 Flow**

Create EVC

The following configuration settings are used to create the EVC.

- VID = 101.
- Learning is enabled because this is a LAN service. NNI port 4 is used.
- Inner tag is C-tag. VID mode is normal. VID = 58.
- PCP = 0. DEI = 0.

EVC ICLI Command

```
# evc 5 vid 101 ivid 101 interface GigabitEthernet 1/4 learning policer none
```

Create EVC Control Entry (ECE) for UNI 1

The following service parameters and actions are used to create the ECE for UNI 1.

Service Parameters

UNI port = 2.

UNI matching VID = 71.

MAC parameters are set to any.

NNI outer tag is allowed to insert a tag on the UNI. This is for uni-directional services only, and it is not used in this case.

Actions

- EVC ID = 5.
- Direction = Both (bi-directional service).
- Tag Pop Count = 1 for ELAN service (all frames are passed to the EVC popping one tag in the direction UNI to NNI and pushing one tag the other direction).
- Policy ID = 0 because this service is not using any policer. The policy ID is used to point to an ACL so that the ACL can then be used to select an EVC policer.

ECE ICLI Command

```
# evc ece 1 interface GigabitEthernet 1/2 outer-tag match type tagged vid 71
inner-tag add type c-tag vid 58 pcp-mode fixed dei-mode fixed evc 5 policer
none pop 1
```

Create EVC Control Entry (ECE) for UNI 2

The following service parameters and actions are used to create the ECE for UNI 2.

Service Parameters

- UNI port = 3.
- UNI matching VID = 81.
- MAC parameters are set to any.
- NNI outer tag is allowed to insert a tag on the UNI. This is for uni-directional services only, and it is not used in this case.

Actions

- EVC ID = 5.
- Direction = Both (bi-directional service).
- Tag Pop Count = 1 for ELAN service (all frames are passed to the EVC popping one tag in the direction UNI to NNI and pushing one tag the other direction).
- Policy ID = 0 because this service is not using any policer. The policy ID is used to point to an ACL so that the ACL can then be used to select an EVC policer.

ECE ICLI Command

```
# evc ece 2 interface GigabitEthernet 1/3 outer-tag match type tagged vid 81
inner-tag add type c-tag vid 58 pcp-mode fixed dei-mode fixed evc 5 policer
none pop 1
```

Directional Services

All services can be configured as uni-directional. Uni-directional services are used where the flows are uni-directional and will save resources compared to a bi-directional service. Also, bi-directional services may need to be configured as two uni-directional services. An example is if the priority is handled different in the two directions.

Create UNI-to-NNI ECE

In the following example, EVC1 is configured using uni-directional service. The EVC configuration is the same as for bi-directional service. The UNI-to-NNI ECE is configured using the following parameters.

Service Parameters

- UNI port = 1.
- UNI matching is any for all to one bundling. MAC parameters are set to any.
- NNI outer tag is allowed to insert a tag on the UNI. This is for uni-directional NNI-UNI service only.

Actions

- EVC ID = 1.
- Direction = UNI-NNI.
- Tag Pop Count = 0 for EPL service (all frames are passed to the EVC without popping any tags).
- Policy ID = 0 because this service is not using any policer. The policy ID is used to point to an ACL so that the ACL can then be used to select an EVC policer.

ICLI Command

```
# evc ece 5 interface GigabitEthernet 1/1 direction uni-to-nni evc 1 policer
none
```

Create NNI-to-UNI ECE

The NNI-to-UNI is configured using the following parameters:

Service Parameters

- UNI 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. The tag is equal to the Outer tag specified for the EVC = 54. The UNI will have added a tag of 54 with PCP and DEI preserved from the EVC's tag.

Actions

- EVC ID = 1.
- Direction = NNI-UNI.
- Tag Pop Count = 0 for EPL service (all frames are passed to the EVC without popping any tags).
- Policy ID = 0 because this service is not using any policer. The policy ID is used to point to an ACL so that the ACL can then be used to select an EVC policer.

ICLI Command

```
# evc ece 5 interface GigabitEthernet 1/1 outer-tag add mode enable vid 60
direction nni-to-uni evc 1 policer none
```

VLAN Port Configuration

The NNI port uses C-tag by default. This can be changed to S-tag or custom S-Tag, as shown in the following commands.

ICLI Command

```
# vlan ethertype s-custom-port 0x9100
# interface GigabitEthernet 1/4
# switchport hybrid port-type s-custom-port
```

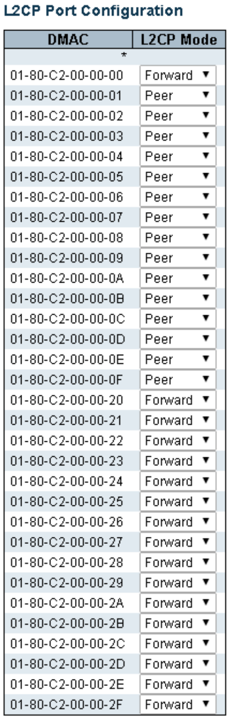
L2CP Handling

L2CP frames can be forwarded or tunneled into the service.

Port Configuration

The following L2CP mode options are available for each DMAC.

- Peer the packet is sent to the protocol stack running in the CPU.
- Forward the packet is forwarded like a normal data packet. ECE rules have to be added to forward this L2CP frame into a service.
- Discard the packet is dropped at the port ingress.



L2CP Port Configuration

DMAC	L2CP Mode
*	
01-80-C2-00-00-00	Forward
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
01-80-C2-00-00-2A	Forward
01-80-C2-00-00-2B	Forward
01-80-C2-00-00-2C	Forward
01-80-C2-00-00-2D	Forward
01-80-C2-00-00-2E	Forward
01-80-C2-00-00-2F	Forward

Figure 7 • **l2CP port configuration**

ICLI Command

```
# interface GigabitEthernet 1/1, 4
# evc l2cp forward 0
```

EPL Service with L2CP Forwarding

ICLI Command

```
# evc 1 vid 21 ivid 21 interface GigabitEthernet 1/4 policer none
```

ECE Rule for Data or L2CP Frames

ICLI Command

```
# evc ece 1 interface GigabitEthernet 1/1 policer none
```

Note: For forwarding/tunneling L2CP frames into the service, the port level configuration for the corresponding L2CP protocol should be set to Forward on UNI and NNI ports.

EVPL Service with L2CP Tunneling

ICLI Command

```
# evc 2 vid 31 ivid 31 interface GigabitEthernet 1/4 policer none
```

ECE Rule for Data Traffic

ICLI Command

```
# evc ece 1 interface GigabitEthernet 1/1 outer-tag match type tagged vid 10
evc 2 policer none policy 12
```

ECE Rule for Tunneling L2CP Traffic

ICLI Command

```
# evc ece 2 lookup advanced interface GigabitEthernet 1/1 frame-type l2cp stp
evc 2 l2cp mode tunnel policer none policy 12
```

Note Policy ID used in ECE rules for data traffic and L2CP traffic should be same for tunneling the L2CP frames. Both rules should be present. EVC Keytype for Advanced Lookup should be Normal->Destination for Tunneling L2CP

Classification and Policing

The classification and policing is shown with four Class of Services policed as follows:

- Cos 0: pbits 0,1: CIR=1Mbps, CBS=64000Bytes, EIR=5Mbps, EBS=64000Bytes.
- Cos 1: pbits 2,3: CIR=5Mbps, CBS=64000Bytes, EIR=5Mbps, EBS=64000Bytes.
- Cos 2: pbits 4,5,6: CIR=5Mbps, CBS=64000Bytes, EIR=5Mbps, EBS=64000Bytes.
- Cos 3: pbits 7: CIR=10Mbps, CBS=64000Bytes, EIR=0, EBS=0.

Bandwidth Configuration

ICLI Commands

```
# evc policer 1 enable cir 1000 cbs 64000 eir 5000 ebs 64000
# evc policer 2 enable cir 5000 cbs 64000 eir 5000 ebs 64000
# evc policer 3 enable cir 5000 cbs 64000 eir 5000 ebs 64000
# evc policer 4 enable cir 10000 cbs 64000
```

Applying Bandwidth Profiles to ECEs on ME1200

Use the following steps to apply bandwidth profiles to ECEs on ME1200.

ICLI Command

```
# evc ece 7 interface GigabitEthernet 1/2 outer-tag match type tagged vid 10
pcp 0-1 evc 2
# evc ece 8 interface GigabitEthernet 1/2 outer-tag match type tagged
vid 10 pcp 2-3 evc 2 policer 2
# evc ece 9 interface GigabitEthernet 1/2 outer-tag match type tagged vid 10
pcp 4-5 evc 2 policer 3
# evc ece 10 interface GigabitEthernet 1/2 outer-tag match type tagged vid 10
pcp 6 evc 2 policer 3
# evc ece 11 interface GigabitEthernet 1/2 outer-tag match type tagged vid 10
pcp 7 evc 2 policer 4
```

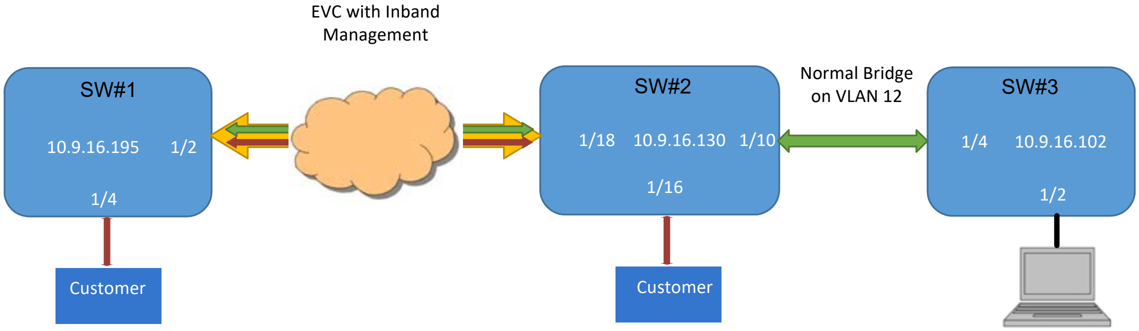
CHAPTER 7

Double VLAN Tag Management Configuration

The standard way to manage a switch is using a single management VLAN. By default all ports are member of the management VLAN (VID = 1), so all ports are able to manage the switch. This Application Note describes how to configure double VLAN tag management. The application for this is remote management over single Ethernet service connection, i.e. management in one VLAN and customer traffic in another VLAN, both carried over the same EVC.

The following illustration shows a sample double VLAN management configuration, which consists of three switches.

Figure 1 • **Sample Configuration**



- Switch 1 is the remote node, managed through a single Ethernet Virtual Connection (EVC) carrying both customer traffic and management.
- Switch 2 is the end point for the EVC where the customer traffic and management VLAN is carried as standard management VLAN to switch 3.
- Customer traffic is sent between switch 1 and switch 2.

Switch 1 Configuration

Step 1 Two EVCs are configured on NNI port 2. Both EVCs have VID = 100, but one with IVID = 100 as normal, while the other has IVID = 12, the management VID.

Step 2 A bi-directional EVC Control Entry (ECE) is configured for customer traffic coming from port 4 with VID = 10,

Step 3 The following steps shows the configuration of two uni-directional ECEs to connect the management VLAN (12).

- UNI-to-NNI adding VID = 100 as outer tag and VID = 12 as inner tag

- NNI-to-UNI matching on same and popping off the two tags

Step 4 Configure IP address on vlan 12.

CLI Configuration for Switch 1

```
evc 1 vid 100 ivid 100 interface GigabitEthernet 1/2 learning policer
none
evc 4 vid 100 ivid 12 interface GigabitEthernet 1/2 learning policer
none
evc ece 4 outer-tag match type c-tagged vid 100 inner-tag match type
c-tagged vid 12 direction nni-to-uni rule-type rx evc 4
evc ece 5 inner-tag add type c-tag vid 12 direction uni-to-nni rule-type
tx evc 4
evc ece 6 interface GigabitEthernet 1/4 outer-tag match type tagged vid
10 policer none policy 1 evc 1
interface vlan 12 ip address 10.9.16.195 255.255.255.0
```

Switch 2 Configuration

CLI Configuration for Switch 2

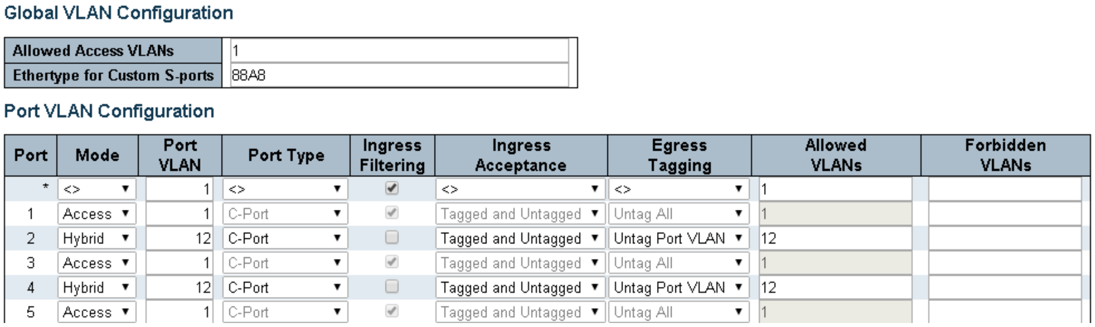
The configuration is same as switch 1, but with port 1 as uni port for management.

```
evc 1 vid 100 ivid 100 interface GigabitEthernet 1/2 learning policer
none
evc 4 vid 100 ivid 12 interface GigabitEthernet 1/2 learning policer
none
evc ece 4 interface GigabitEthernet 1/1 outer-tag match type c-tagged
vid 100 inner-tag match type c-tagged vid 12 direction nni-to-uni
rule-type rx evc 4 pop 2
evc ece 5 interface GigabitEthernet 1/1 inner-tag add type c-tag vid 12
direction uni-to-nni evc 4
evc ece 6 interface GigabitEthernet 1/4 outer-tag match type tagged vid
10 policer none policy 1
```

Switch 3 Configuration

Switch 3 is configured with an IP address on the same subnet as switch 1. It is used to verify management connectivity, as shown in the following illustration.

Figure 2 • **VLAN Configuration**



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	Hybrid	12	C-Port	□	Tagged and Untagged	Untag Port VLAN	12	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Hybrid	12	C-Port	□	Tagged and Untagged	Untag Port VLAN	12	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

CLI Configuration for Switch 3

```
interface vlan 12 ip address 10.9.16.102 255.255.255.0
interface GigabitEthernet 1/2,4 no loop-protect
switchport hybrid native vlan 12 switchport hybrid allowed vlan 12
switchport mode hybrid
```

CHAPTER 8

Service OAM Configuration

This document shows how to set up Service OAM (Y.1731 and IEEE802.1ag) using the Industrial Command Line Interface (ICLI) commands. The Service OAM model on the ME1200 is outlined to describe the possible configurations.

This document is based on the ICLI Configuration guide that describes the basic usage of the ICLI and the Service OAM reference guide that describes the Service OAM ICLI commands.

The following sections explain the OAM Model with a few configuration examples.

Understanding Service OAM

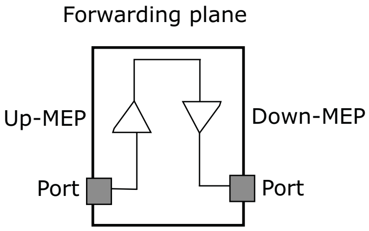
Service OAM is based on the IEEE 802.1ag and Y.1731 standards. Based upon these standards, the Metro Ethernet Forum has defined the MEF17 standard, which specifies the requirements and framework for Service OAM within MEF compliant Metro Ethernet networks.

The service OAM mechanism enables point-to-point or point-to-multi point Fault Management (FM) and Performance Monitoring (PM) in an Ethernet network using Maintenance End Points (MEP) and Maintenance Intermediate Points (MIP) as the building blocks.

- An MEP can be either an up-MEP or a Down-MEP.
- A Down-MEP is injecting/terminating OAM against a port.
- An up-MEP is injecting/terminating OAM against the forwarding plane.

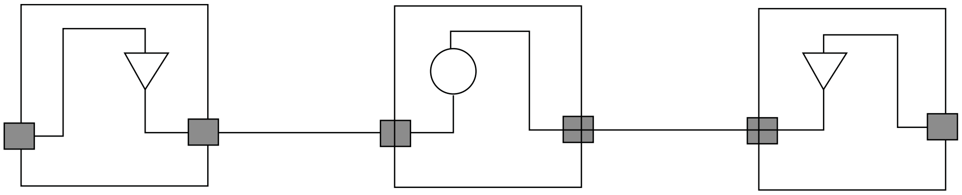
In the following illustrations, MEP is represented by a triangle and MIP by a circle.

Figure 1 • **Maintenance End Points**



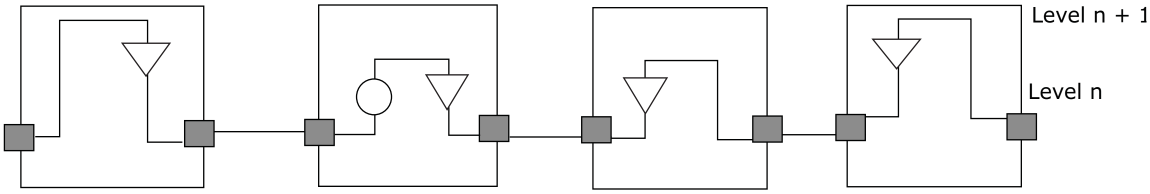
In a flow, at least two MEPs exchange OAM PDU to achieve the FM and PM functionality. A number of MEPs in the same flow can form a group called a Maintenance Entity Group (MEG).

Figure 2 • **Maintenance Entity Group**



In a flow, all MEPs in an MEG are on the MEG's level. Multiple MEGs can be nested in a flow in such a manner that an MEG on a higher level is able to encapsulate an MEG on a lower level. The lower level MEG is transparent to the higher level MEG PDU.

Figure 3 • **Nested Maintenance Entity Group**



Note: Before starting the ICLI configuration, please prepare a serial RS-232 cable and terminal console software for accessing the device on the management platform. Please refer to Chapter 4.

Service OAM Model

In the OAM model, an MEP instance can be created in three different domains.

- Port: associated with a port
- VLAN: associated with a VLAN
- EVC: associated with an EVC

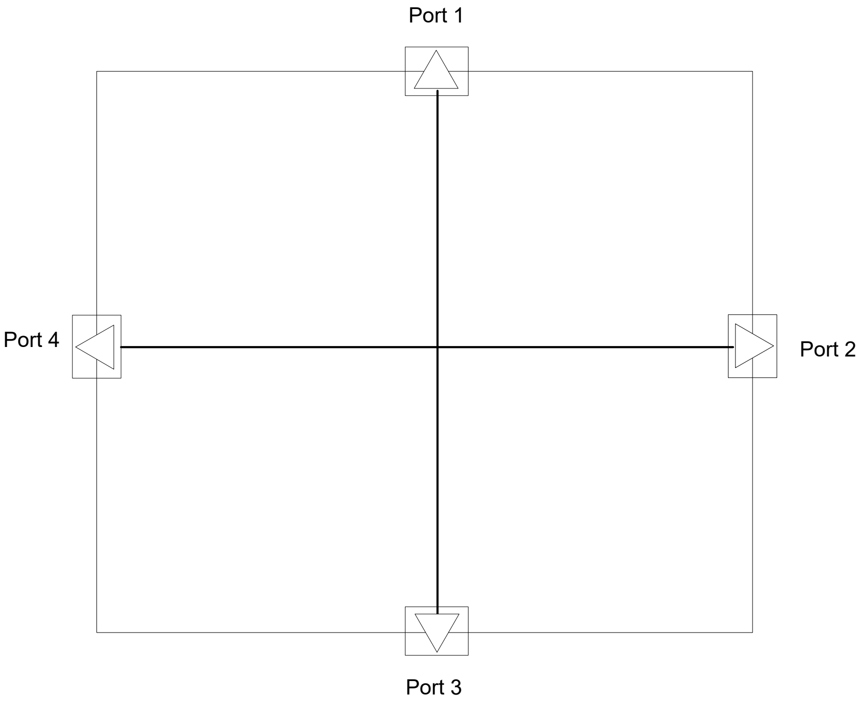
On a classified VID, only one OAM domain can exist. As both VLAN and EVC use a classified VID, EVC OAM and VLAN OAM cannot coexist on the same VID.

Note Multiple MEPs in the same domain have shared MEG level. Multiple MEPs in different domains have independent MEG levels.

Port OAM

The following illustration shows MEPs created in the port domain. MEPs can also be created in VLAN and EVC domains.

Figure 4 • **Port Domain Model**

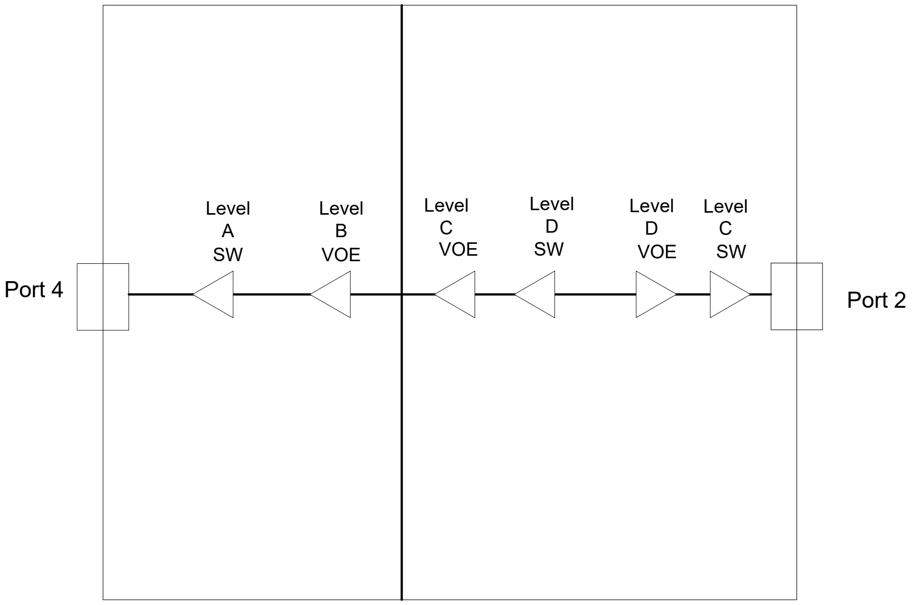


- An MEP can be created on any port as either a software-based or OAM Engine (VOE)-based MEP.
- The port domain is untagged.

VLAN OAM

The following illustration shows a VLAN MEP configuration. This is in addition to the port domain MEPs.

Figure 5 • **VLAN Domain Model**

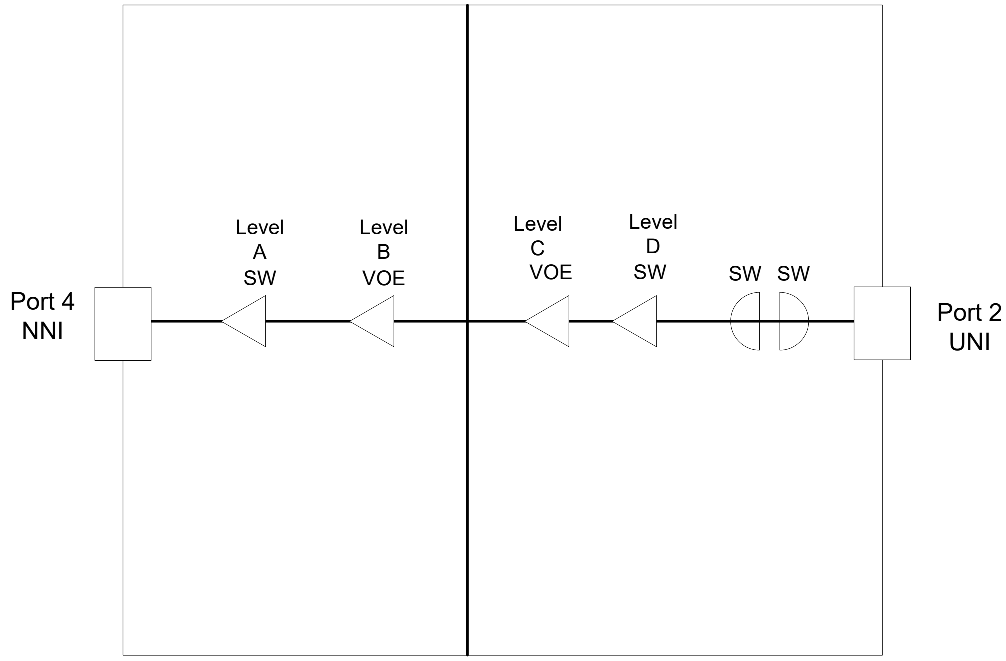


- VLAN MEPs configured on the same VLAN have shared MEG levels.
- VLAN OAM is only supported in a two-port VLAN, such as a VLAN based E-Line.
- Up-MEP can be configured on one port only.
- Down-MEP can be configured on both ports.
- For each possible up/down-MEP, one software and one VOE based MEP can be configured.
- VOE down-MEP is on a higher level than software down-MEP.
- VOE up-MEP is on a lower level than software up-MEP.
- Down-MEP is on a lower level than up-MEP

EVC OAM

The following illustration shows an EVC MEP configuration. This is in addition to the port domain MEPs.

Figure 6 • **EVC Domain Model**



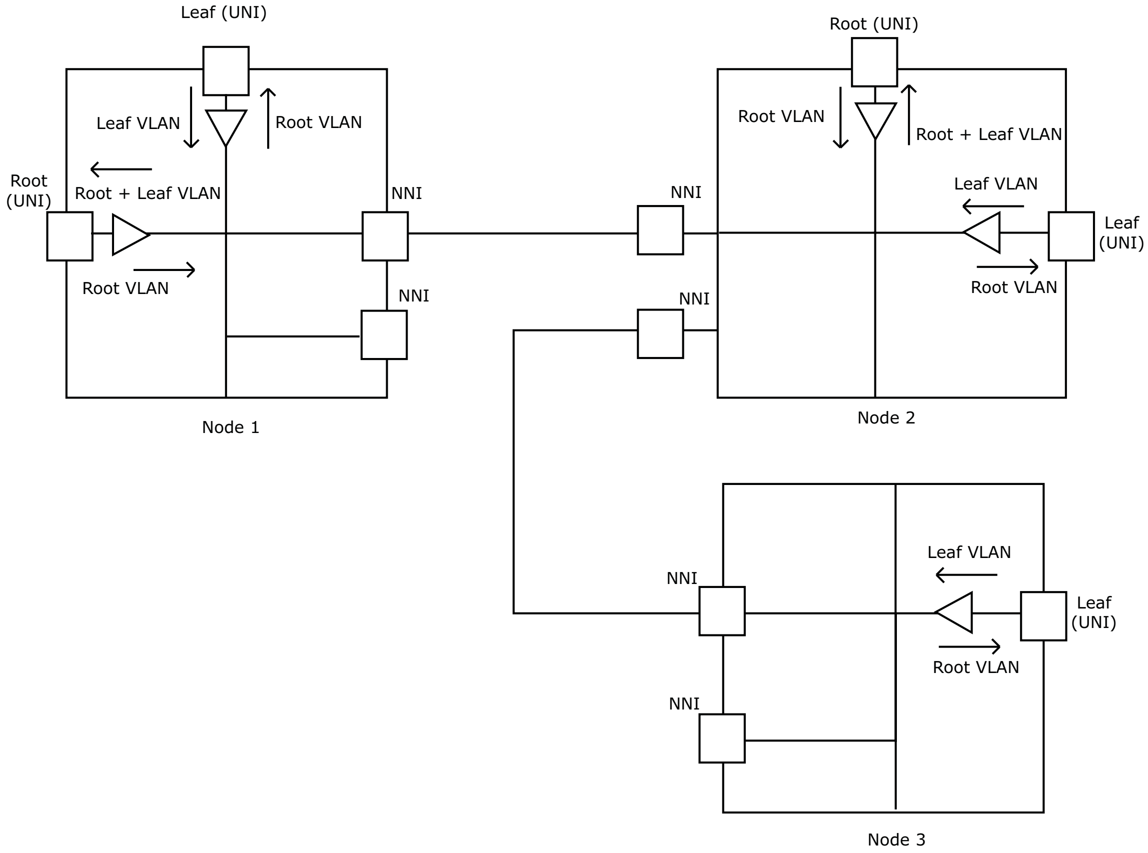
- EVC MEPs configured in the same EVC have shared MEG levels.
- EVC OAM is only supported in an E-Line.
- There is only EVC up-MEP on the UNI port. There is only MIP on UNI. This is a subscriber flow MIP that belongs to a subscriber MEG, and not the EVC MEG.
- There is no EVC down-MEP on a port with EVC up-MEP.
- There is one VOE and one software-based MEP on each port.
- VOE down-MEP is on a higher level than software down-MEP.
- VOE up-MEP is on a lower level than software up-MEP.
- Down-MEP is on a lower level than up-MEP.

E-TREE

An E-Tree is a special configuration of an EVC. In an E-Tree all UNIs are either a root or leaf UNI. Service frames arriving on a leaf UNI can only be forwarded to root UNIs. Service frames arriving on a root UNI can be forwarded to other root UNIs or to leaf UNIs.

An EVC up-MEP created on a root UNI becomes a root MEP. An EVC up-MEP created on a leaf UNI becomes a leaf MEP. The following illustration shows how the root and leaf MEPs inject and extract frames in different VLANs.

Figure 7 • **E-TREE Model**



A root MEP has all root/leaf MEPs as peers and a leaf MEP has all root MEPs as peers.

It is only possible to have UNI software up-MEP in an E-Tree. In case of more up-MEP in same E-Tree, they must all be on the same level.

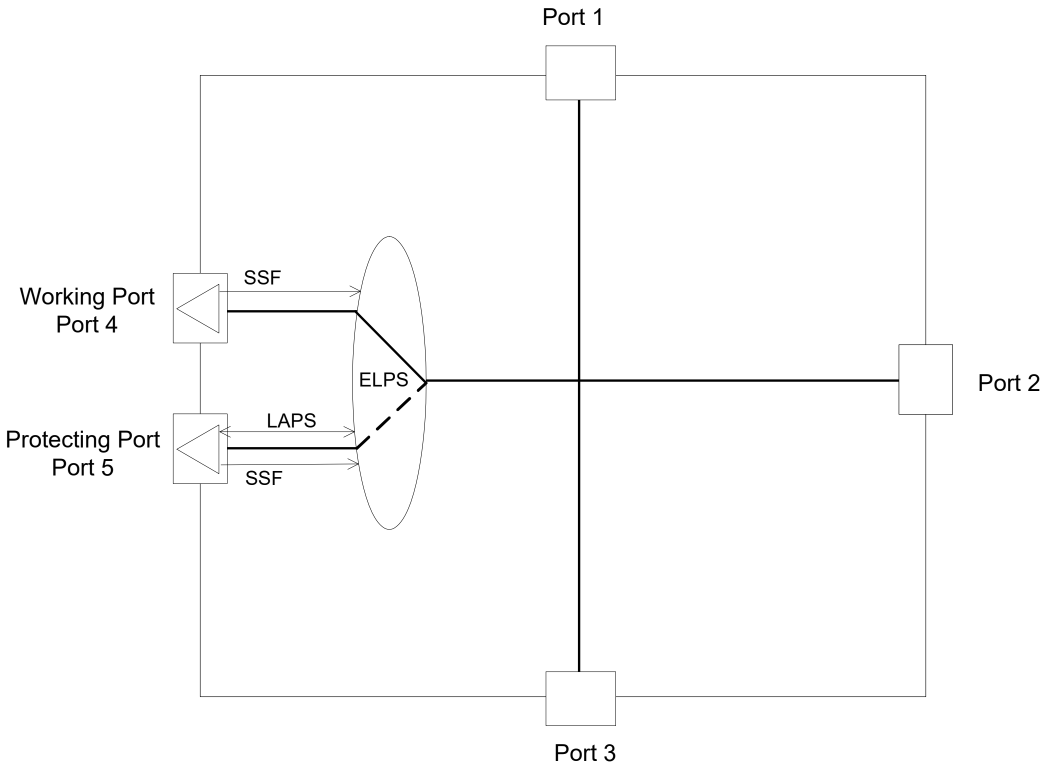
Port Protection

Port protection is a linear protection according to G.8031.

Basic Port Protection Model

A port domain Ethernet Linear Protection Switching (ELPS) instance protects all classified VID on a (working) port. The classified VID can be related to either a VLAN or an EVC.

Figure 8 • **Basic Port Protection Model**



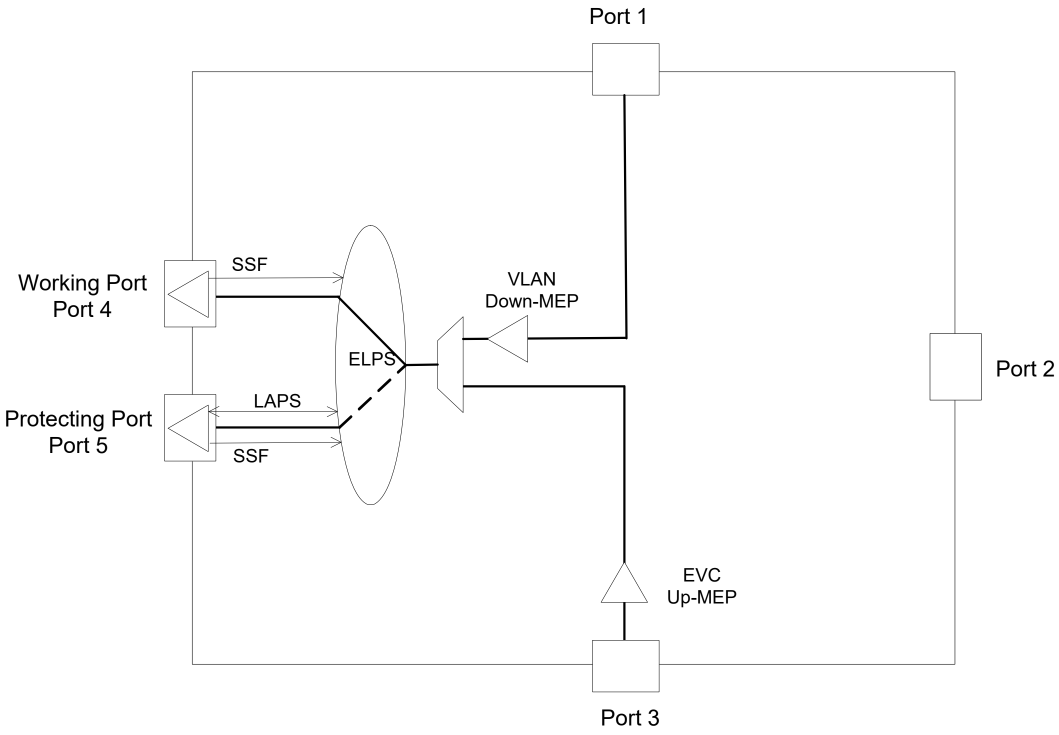
- Port ELPS requires a working and protecting port MEP for Server Signal Fail (SSF) calculation based on continuity check and link state (G.8021), and for LAPS <-> APS PDU conversion.
- LAPS protocol information is handled by the ELPS function as specified in G.8031(11/2009).
- VLAN OAM and EVC OAM models can be protected by this ELPS.

Port Protection with Service OAM

The protected classified VID can be related to either a VLAN or an EVC, and each of these can have MEPs configured. The following illustration shows a port ELPS protecting two different classified VIDs,

one related to a VLAN and another related to an EVC. In the VLAN a down-MEP is configured and in the EVC an up-MEP is configured.

Figure 9 • **Port Protection with Service OAM**



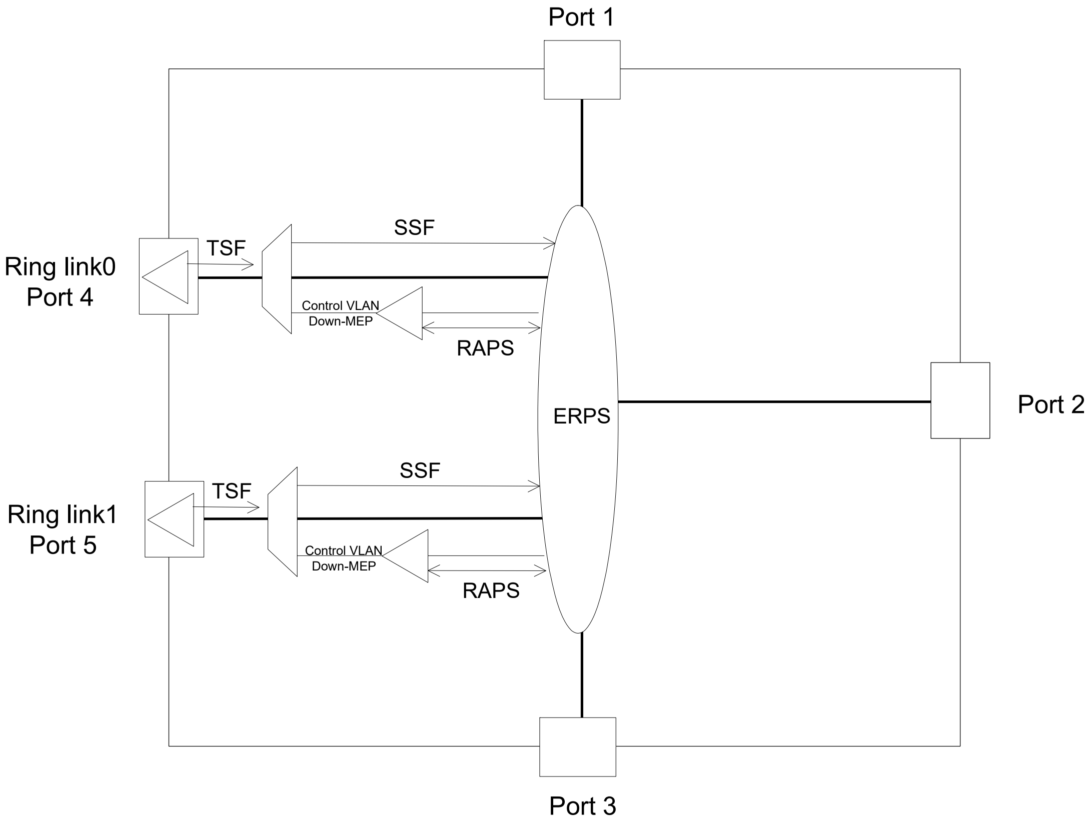
Ring Protection

Ring protection is a VLAN protection according to G.8032.

Basic Ring Protection Model

An Ethernet Ring Protection Switching (ERPS) instance protects the configured classified VIDs, as a node in a ring topology, through the two ring links 0/1.

Figure 10 • **Basic Ring Protection Model**



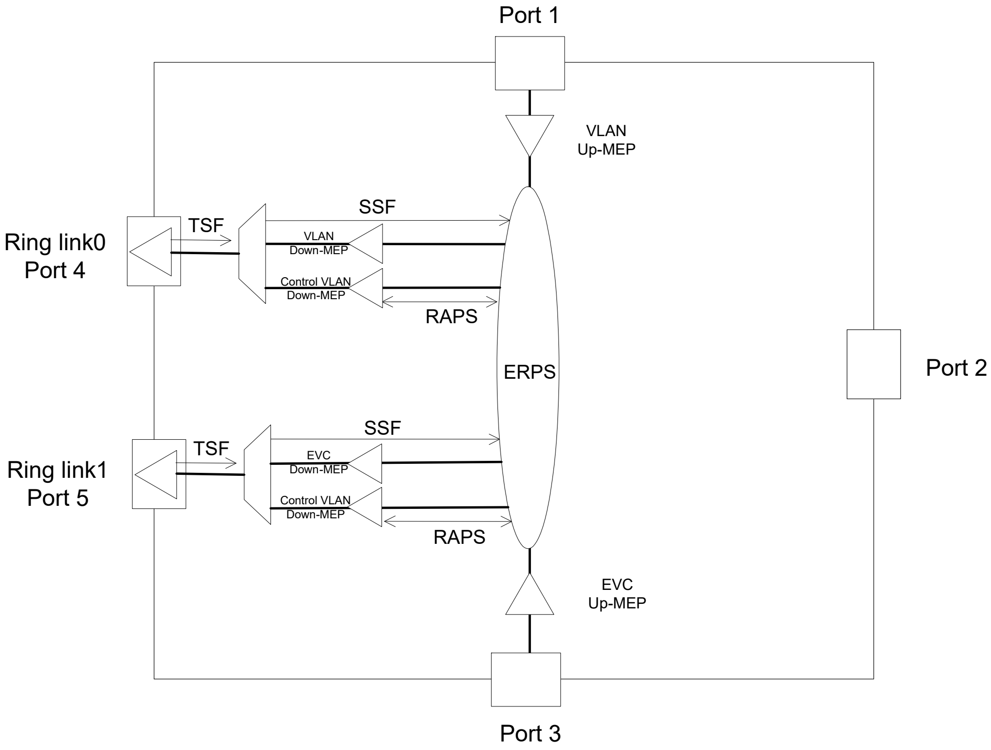
- Ring link0 and link1 are ports. The ERPS requires a port MEP on link0 and link1 port for SSF calculation based on continuity check and link state (G.8021). It also requires a control VLAN down-MEP on link0 and link1 port for RAPS <-> APS PDU conversion.
- The RAPS protocol information is handled by the ERPS function as specified in G.8032(03/2010).
- VLAN OAM and EVC OAM models can be protected by this ERPS.

Ring Protection with Service OAM

Protected classified VIDs can be related to either a VLAN or an EVC, and each of these can have MEPs configured. The following illustration shows an ERPS protecting two different classified VIDs, one related to a VLAN and the other related to an EVC. In the VLAN and the EVC, both a down-MEP and an up-MEP are configured.

Note VLAN/EVC down-MEPs are not protected by the ring. These are segment MEPs that can cover a section of a ring, if desired.

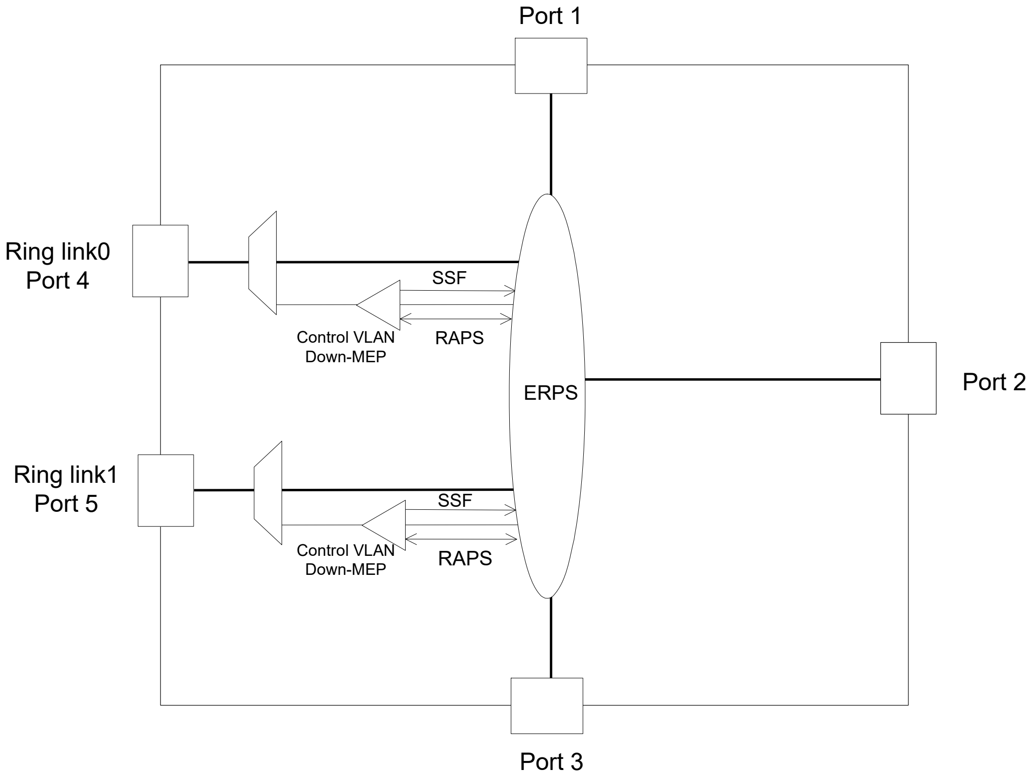
Figure 11 • **Ring Protection with Service OAM**



Alternative SSF Source

According to G.8032 the Signal Fail can be taken from a test trail. In the Cisco solution it is possible to take SSF from any created MEP instance. The following illustration shows that the control VLAN down-MEP calculates the SSF to enable multiple ring instances per port using independent continuity check functions (SSF generation).

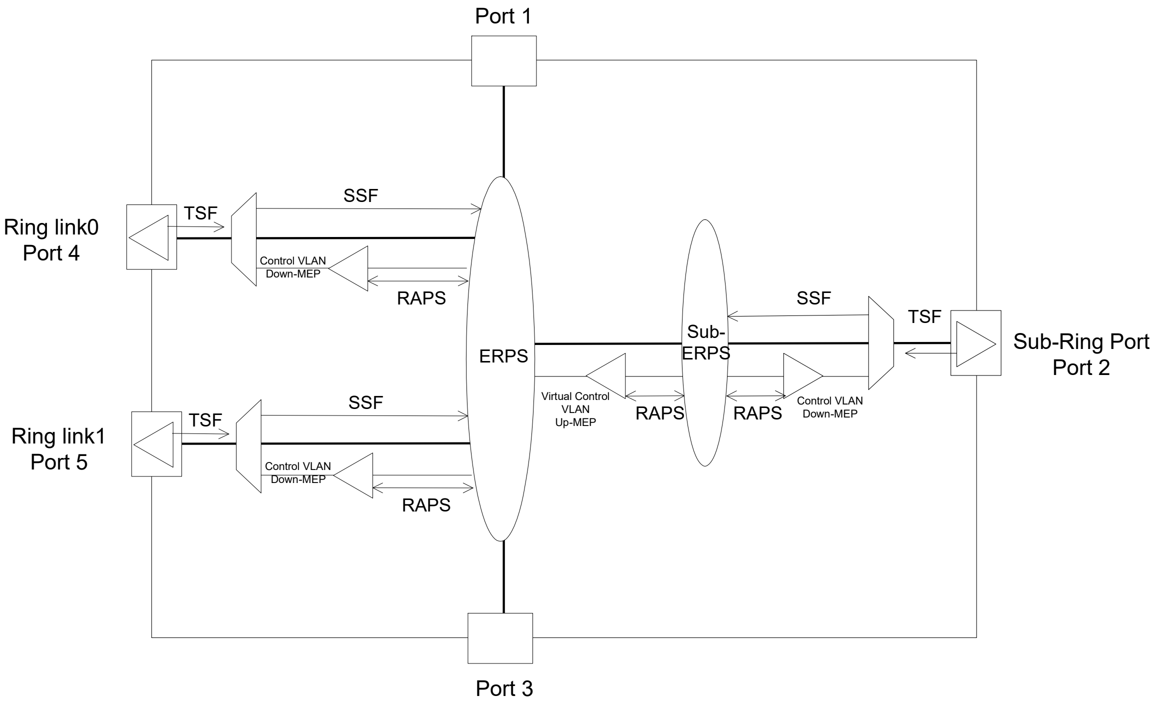
Figure 12 • **Alternative SSF Source**



Ring Interconnection Protection

In the following illustration, the virtual channel RAPS is handled by a control VLAN up-MEP resident on the sub-ring port. The ring interconnected ring model can be with or without virtual control channel through major ring.

Figure 13 • **Ring Interconnection Protection**



- The sub-ring link is a port. The sub-ERPS instance requires a port MEP on sub-ring link port for SSF calculation based on continuity check and link state (G.8021). It also requires a control VLAN down-MEP on sub-ring port for RAPS <-> APS PDU conversion.
- The virtual control VLAN up-MEP used for RAPS handling must be a softare-based MEP.

Service OAM Configuration Examples

This section describes ICLI configuration examples. For more information about the models, see Service OAM Model.

Restore Default Setup using CLI

Use the following commands to restore default settings before starting to configure any of the examples in the following sections.

1. Initiate MEP Configuration and Ensure IS1 Key Type

```
(config)# interface GigabitEthernet 1/1-5
(config-if)# evc key double-tag
(config-if)# exit
#
```

Display all MEP Commands and Parameters

```
! Show all MEP related ‘configuration’ commands
# configure terminal
(config)# mep ??
mep <inst> [mip] {up | down}
           domain {port | evc | vlan | tp-link | tunnel-tp | pw | lsp}
[vid <vid>]
```

```
           [flow <flow>] level <level> [interface <port_type> <port>]
mep <inst> ais [fr1s | fr1m] [protect]
mep <inst> aps <prio> [multi | uni] {laps | {raps [octet <octet> ]}}
mep <inst> bfd cc-period <cc_period>
         [mode {coordinated | independent rx-flow <rx_flow>}] [cc-only]
           [tx-auth key <tx_key_id>] [rx-auth]
mep <inst> cc <prio> [fr300s | fr100s | fr10s | fr1s | fr6m | fr1m | fr6h]
mep <inst> ccm-tlv
mep <inst> client domain {evc | vlan | lsp} flow <cflow> [level <level>]
           [ais-prio [<aisprio> | ais-highest]]
           [lck-prio [<lckprio> | lck-highest]]
mep <inst> dm bin-number { fd | ifdv } <number>
mep <inst> dm bin-range { fd | ifdv } <list_1> <range_1> [ <list_2>
<range_2> ] [ <list_3> <range_3> ] [ <list_4> <range_4> ]
mep <inst> dm bin fd <num_fd_var>
mep <inst> dm bin ifdv <num_ifdv_var>
mep <inst> dm bin threshold <threshold_var>
mep <inst> dm ns
mep <inst> dm overflow-reset
mep <inst> dm proprietary
mep <inst> dm syncronized
mep <inst> lb <prio> [dei]
           [multi | {uni {{mep-id <mepid>} | {mac <mac>}}} | mpls ttl
<mpls_ttl>]
           count <count> size <size> interval <interval>
mep <inst> lck [fr1s | fr1m]
mep <inst> level <level>
mep <inst> link-state-tracking
mep <inst> lm <prio> [multi | uni] [single | dual]
           [fr10s | fr1s | fr6m | fr1m | fr6h] [flr <flr>]
mep <inst> lm flow-counting
mep <inst> lm oam-counting {[y1731 | all]}
mep <inst> lm-avail interval <interval-number> flr-threshold
<threshold-limit>
mep <inst> lm-avail maintenance
mep <inst> lt <prio> {{mep-id <mepid>} | {mac <mac>}} ttl <ttl>
mep <inst> meg-id <megid> {itu | itu-cc | {ieee [name <name>]}}
mep <inst> mep-id <mepid>
mep <inst> peer-mep-id <mepid> [mac <mac>]
mep <inst> performance-monitoring
mep <inst> rt <tc> [src-id-tlv] [dst-id-tlv] [pad-tlv type {drop | copy}
           length <pad_tlv_len>] [flags {[V] [T] [R]}] [ttl <ttl_val>]
mep <inst> syslog
mep <inst> tst <prio> [dei] mep-id <mepid> [sequence]
           [all-zero | all-one | one-zero] rate <rate> size <size>
mep <inst> tst rx
mep <inst> tst tx
mep <inst> vid <vid>
mep <inst> voe
mep bfd auth-key <key_id> {simple-pwd | md5 | sha1} key <auth_key>
mep os-tlv oui <oui> sub-type <subtype> value <value>
(config) #
```

Get MEP Status and Configuration Overview

```
! Show all MEP related ‘show’ commands
# sh mep ?
```

```
show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client |
ais | lck | pm | syslog |
                   tlv | bfd | rt | lst] [detail]
show mep bfd-auth-key [ <inst> ]
```

Show Command

```
! Show status of all enabled MEP
# show mep
MEP state is:
  Inst  cLevel  cMeg  cMep  cAis  cLck  cSsf  aBlk  aTsf  Peer MEP  cLoc
cRdi  cPeriod  cPrio
    11   False False False False False  True False  True        3 False
False    False  False

! Show status and configuration of all enabled MEP
# show mep detail
MEP state is:
  Inst  cLevel  cMeg  cMep  cAis  cLck  cSsf  aBlk  aTsf  Peer MEP  cLoc
cRdi  cPeriod  cPrio
    11   False False False False False  True False  True        3 False
False    False  False

MEP Basic Configuration is:
  Inst  Mode  Voe  PM  Vola  Direct                Port   Dom  Level
Format
    11   Mep  Voe             Down    GigabitEthernet 1/2  Port      2
IEEE String

! Show configuration of a selected 'feature'
# show mep cc detail

MEP CC Configuration is:
     Inst     Prio       Rate
       11        4         1s
```

Port OAM Configuration

According to the Port OAM service model a down-MEP can be created on a port.

Use the following parameters to create a VOE-based port domain down-MEP.

```
Instance number:  1
Residence port:   Gigabit Ethernet port 4
Level:            0
MEG format:       ITU
MEG-ID:           ICC000MEG0001
MEP-ID:           1
Peer MEP-ID:      2
```

Continuity check is enabled on priority 0 at rate 300 f/s.

Configure Port Domain OAM Down-MEP using CLI

1. Enable the MEP instance.

```
(config)# mep 1 down domain port level 0 interface GigabitEthernet 1/4
```

2. Configure the MEG-ID.

```
(config)# mep 1 meg-id ICC000MEG0001 itu
```

3. Configure the MEP-ID.

```
(config)# mep 1 mep-id 1
```

4. Make it VOE-based.

```
(config)# mep 1 voe
```

5. Configure a peer MEP.

```
(config)# mep 1 peer-mep-id 2
```

6. Enable Continuity check.

```
(config)# mep 1 cc 0 fr300s
```

7. Run the following commands to verify the configuration.

```
(config)# do show running-config
[...]
mep os-tlv oui 0xC sub-type 0x1 value 0x2
mep 1 down domain port level 0 interface GigabitEthernet 1/4
mep 1 meg-id ICC000MEG0001 itu
mep 1 voe
mep 1 peer-mep-id 2
mep 1 cc 0 fr300s
[...]
(config)# do show mep detail
MEP state is:
  Inst cLevel  cMeg  cMep  cAis  cLck  cSsf  aBlk  aTsf  Peer MEP  cLoc
cRdi  cPeriod  cPrio
     1  False False False False False  True False  True         2 False
False    False  False
MEP Basic Configuration is:
  Inst  Mode  Voe  Direct   Port   Dom  Level   Format     Meg id
Mep id   Flow
    1  Mep  Voe   Down    1/4    Port    0  ITU ICC  ICC000MEG0001
1     4
(config)# do show mep cc detail
MEP CC Configuration is:
     Inst     Prio       Rate
        1        0       300s
```

VLAN OAM Configuration

According to the VLAN OAM service model both up- and down-MEP can be created in a VLAN. Before up- or down-MEP is created, create VLAN. A VLAN 111 is created with port members 1 and 4.

Configure Global VLAN using CLI

1. Create the VLAN 111

```
(config)# vlan 111
```

2. Make port 1 and 4 member of VLAN 111.

```
(config-vlan)# interface GigabitEthernet 1/1,4
(config-if)# switchport hybrid allowed vlan 111
(config-if)# switchport mode hybrid
(config-if)# exit
```

In VLAN 111 a down-MEP can be created.

Use the following parameters to create a VOE-based VLAN domain down-MEP.

```
Instance number: 2
Residence port:  Gigabit Ethernet port 4
```

```
Level:            0
MEG format:       ITU
MEG-ID:           ICC000MEG0001
MEP-ID:           1
Peer MEP-ID:      2
```

Continuity check is enabled on priority 7 at rate 1 f/s.

Configure VLAN Domain OAM Down-MEP using CLI

1. Enable the MEP instance.

```
(config)# mep 2 down domain vlan flow 111 level 0 interface
GigabitEthernet 1/4
```

2. Configure the MEG-ID.

```
(config)# mep 2 meg-id ICC000MEG0001 itu
```

3. Configure the MEP-ID.

```
(config)# mep 2 mep-id 1
```

4. Make it VOE-based.

```
(config)# mep 2 voe
```

5. Configure a peer MEP.

```
(config)# mep 2 peer-mep-id 2
```

6. Enable Continuity check.

```
(config)# mep 2 cc 7 fr1s
```

7. Run the following commands to verify the configuration.

```
(config)# do show running-config
[...]
mep os-tlv oui 0xC sub-type 0x1 value
mep 2 down domain vlan flow 111 level 0 interface GigabitEthernet 1/4
mep 2 meg-id ICC000MEG0001 itu
mep 2 voe
mep 2 peer-mep-id 2
mep 2 cc 7
[...]
(config)# do show mep detail
MEP state is:
  Inst  cLevel  cMeg  cMep  cAis  cLck  cSsf  aBlk  aTsf  Peer MEP  cLoc
cRdi  cPeriod  cPrio
     2   False False False False False  True False  True        2 False
False    False  False
MEP Basic Configuration is:
  Inst  Mode  Voe  Direct   Port   Dom  Level   Format    Meg id
Mep id   Flow
    2  Mep  Voe   Down   1/4   Vlan    0  ITU ICC  ICC000MEG0001
1    111
(config)# do show mep cc detail
MEP CC Configuration is:
     Inst     Prio       Rate
        2        7         1s
```

In VLAN 111 an up-MEP can be created.

Use the following parameters to create a VOE-based VLAN domain up-MEP.

```
Instance number: 3
Residence port:  Gigabit Ethernet port 1
Level:           3
MEG format:      IEEE
Domain Name:     DOMAIN000
MEG-ID:          ICC000MEG0001
```

```
MEP-ID:          1
Peer MEP-ID:     2
```

Continuity check is enabled on priority 7 at rate 300 f/s.

Configure VLAN Domain OAM Up-MEP using CLI

```
# configure terminal
! Enable the MEP instance
(config)# mep 3 up domain vlan flow 111 level 3 interface
GigabitEthernet 1/1
! Configure the MEG-ID
(config)# mep 3 meg-id IEEE000MEG0001 ieee name DOMAIN000
! Configure the MEP-ID
(config)# mep 3 mep-id 1
! Make it VOE-based
(config)# mep 3 voe
! Configure a peer MEP
(config)# mep 3 peer-mep-id 2
! Enable Continuity check
(config)# mep 3 cc 7 fr300s
```

Run the following commands to verify the configuration.

```
(config)# do show running-config
[...]
mep 3 up domain vlan flow 111 level 3 interface GigabitEthernet 1/1
mep 3 meg-id IEEE000MEG0001 ieee name DOMAIN000
mep 3 voe
mep 3 peer-mep-id 2
mep 3 cc 7 fr300s
[...]
(config)# do show mep detail
MEP state is:
  Inst  cLevel  cMeg  cMep  cAis  cLck  cSsf  aBlk  aTsf  Peer MEP  cLoc
cRdi  cPeriod  cPrio
     3   False False False False False  True False  True        2 False
False    False  False
MEP Basic Configuration is:
  Inst  Mode  Voe  Direct   Port   Dom  Level   Format      Name      Meg
id       Mep id  Flow
     3   Mep  Voe     Up    1/1    Vlan     3  IEEE String  DOMAIN000
IEEE000MEG0001     1   111
(config)# do show mep cc detail
MEP CC Configuration is:
     Inst     Prio       Rate
        3        7       300
```

EVC OAM Configuration

According to the EVC OAM service model both up- and down-MEP can be created in an EVC.

Configure an EVC Instance using CLI

Use the following steps to create an EVC instance 1 with port 4 as NNI, port 3 as UNI, and 222 as internal VID.

1. Create the EVC.

```
evc 1 vid 222 ivid 222 interface GigabitEthernet 1/4
```

2. Map any frame on UNI to COS 4 in the EVC.

```
evc ece 1 interface GigabitEthernet 1/3 outer-tag add
pcp-mode mapped pcp 4 cos 4
```

Set UNI PVID to Unused VLAN using CLI

Use the following steps to set UNI PVID to an unused VLAN to discard non-classified frames, exclude UNI port from the VLAN OAM VID, and configure UNI as C-port.

1. Change to interface 3 (UNI) sub-mode.

```
interface GigabitEthernet 1/3
```

2. Set the port based classified VID to an unused value.

```
switchport hybrid native vlan 4095
```

3. Exclude this port from the VLAN OAM VID.

```
switchport forbidden vlan add 111
```

4. Make the UNI a C port.

```
switchport hybrid port-type c-port
```

5. Make the UNI a hybrid port.

```
switchport mode hybrid
```

Set NNI PVID to Unused VLAN using CLI

Use the following steps to set the NNI PVID to an unused VLAN to discard non-classified frames and

configure NNI as S-port.

1. Change to interface 4 (NNI) sub-mode.

```
interface GigabitEthernet 1/4
```

2. Set the port based classified VID to an unused value.

```
switchport hybrid native vlan 4095
```

3. Make the NNI an S port.

```
switchport hybrid port-type s-port
```

4. Make the NNI a hybrid port.

```
switchport mode hybrid
```

Enable Ingress Mapping from PCP to CoS on UNI and NNI using CLI

Use the following steps to enable ingress one-to-one mapping from PCP to CoS on UNI and NNI.

1. Change to interface 3,4 sub-mode.

```
interface GigabitEthernet 1/3,4
```

2. Set Trust configuration.

```
qos trust tag
```

3. Configure PCP and DEI mapping to one-to-one.

```
qos map tag-cos pcp 0 dei 0 cos 0 dpl 0
qos map tag-cos pcp 0 dei 1 cos 0 dpl 1
qos map tag-cos pcp 1 dei 0 cos 1 dpl 0
qos map tag-cos pcp 1 dei 1 cos 1 dpl 1
```

```
exit
```

Enable Ingress Mapping from CoS to PCP on UNI and NNI using CLI

Use the following steps to enable ingress one-to-one mapping from CoS to PCP on UNI and NNI.

1. Change to interface 3,4 sub-mode.

```
interface GigabitEthernet 1/3,4
```

2. Set Tag remarking configuration.

```
qos tag-remark mapped
```

3. Configure PCP and DEI mapping to one-to-one.

```
qos map cos-tag cos 0 dpl 0 pcp 0 dei 0
qos map cos-tag cos 0 dpl 1 pcp 0 dei 1
qos map cos-tag cos 1 dpl 0 pcp 1 dei 0
qos map cos-tag cos 1 dpl 1 pcp 1 dei 1
exit
```

In EVC 1 a down-MEP can be created.

Use the following parameters to create a software-based EVC domain down-MEP.

```
Instance number: 4
Residence port:  Gigabit Ethernet port 4
Level:           0
MEG format:      ITU
MEG-ID:          ICC000MEG0001
MEP-ID:          1
Peer MEP-ID:     2
```

Continuity check is enabled on priority 4 at rate 1 f/s.

EVC Domain OAM Down-MEP Configuration using CLI

Use the following steps to configure EVC domain OAM down-MEP.

1. Enable the MEP instance.

```
mep 4 down domain evc flow 1 level 0 interface GigabitEthernet 1/4
```

2. Configure the MEG-ID.

```
mep 4 meg-id ICC000MEG0001 itu
```

3. Configure the MEP-ID.

```
mep 4 mep-id 1
```

4. Configure a peer MEP.

```
mep 4 peer-mep-id 2
```

5. Enable continuity check.

```
mep 4 cc 4 fr1s
```

Run the following commands to verify the configuration

```
(config)# do show running-config
[...]
mep 4 down domain evc flow 1 level 0 interface GigabitEthernet 1/4
mep 4 meg-id ICC000MEG0001 itu
mep 4 peer-mep-id 2
mep 4 cc 4
 [...]
(config)# do show mep detail
MEP state is:
  Inst  cLevel  cMeg  cMep  cAis  cLck  cSsf  aBlk  aTsf  Peer MEP  cLoc
cRdi  cPeriod  cPrio
```

```
     4   False False False False False  True False  True        2 False
False    False  False
MEP Basic Configuration is:
  Inst  Mode  Voe  Direct   Port   Dom  Level   Format      Meg id
Mep id  Flow
    4   Mep       Down    1/4    Evc     0   ITU ICC    ICC000MEG0001
1      1
(config)# do show mep cc detail
MEP CC Configuration is:
     Inst     Prio       Rate
        4        4         1s
```

In EVC 1 an up-MEP can be created. Use the following parameters to create a VOE-based EVC domain up-MEP.

```
Instance number: 5
Residence port:  Gigabit Ethernet port 3
Level:           7
MEG format:      IEEE
Domain Name:     DOMAIN000
MEG-ID:          IEEE000MEG0001
MEP-ID:          1
Peer MEP-ID:     2
```

Continuity check is enabled on priority 4 at rate 300 f/s.

EVC Domain OAM Up-MEP Configuration using CLI

Use the following steps to configure a VOE based EVC domain OAM up-MEP.

1. Enable the MEP instance.

```
(config)# mep 5 up domain evc flow 1 level 7 interface GigabitEthernet
1/3
```

2. Configure the MEG-ID.

```
(config)# mep 5 meg-id ICC000MEG0001 ieee name DOMAIN000
```

3. Configure the MEP-ID.

```
mep 5 mep-id 1
```

4. Make MEP-ID VOE based.

```
mep 5 voe
```

5. Configure a peer MEP.

```
mep 5 peer-mep-id 2
```

6. Enable continuity check.

```
mep 5 cc 4 fr300s
```

Run the following commands to verify the configuration.

```
(config)# do show running-config
[...]
mep 5 up domain evc flow 1 level 7 interface GigabitEthernet 1/3
mep 5 meg-id ICC000MEG0001 ieee name DOMAIN000
mep 5 voe
mep 5 peer-mep-id 2
mep 5 cc 4 fr300s
[...]
(config)# do show mep detail
MEP state is:
  Inst  cLevel  cMeg  cMep  cAis  cLck  cSsf  aBlk  aTsf  Peer MEP  cLoc
cRdi  cPeriod  cPrio
     5   False False False False False  True False  True        2 False
False    False  False
```

```
MEP Basic Configuration is:
  Inst  Mode  Voe  Direct   Port   Dom  Level   Format      Name      Meg
id       Mep id  Flow
     5   Mep  Voe     Up    1/3    Evc     7  IEEE String  DOMAIN000
IEEE000MEG0001     1      1
(config)# do show mep cc detail
MEP CC Configuration is:
     Inst     Prio       Rate
```

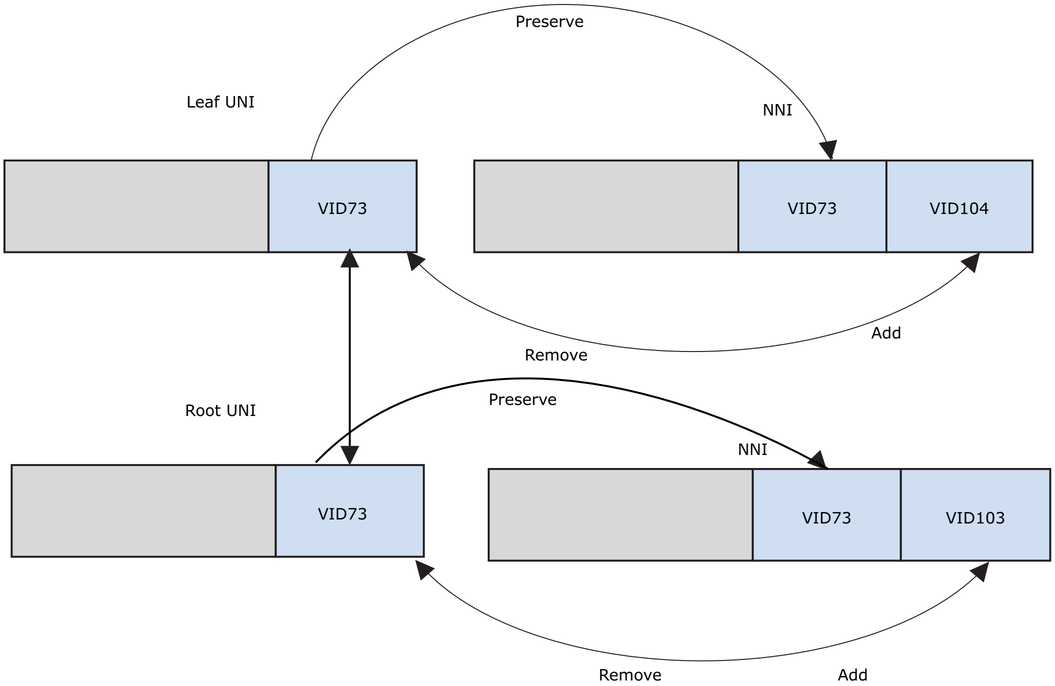
E-TREE OAM Configuration Example

Configure E-TREE OAM using CLI

This section shows the commands used to complete the following tasks.

1. Set up an E-tree service (no-bundling) on a leaf UNI (port 2) for CEVLAN ID 73.
2. Set up an E-tree service (no-bundling) on a root UNI (port 3) for CEVLAN ID 73.
3. On NNI egress, add one tag: outer VID = 103 (loot), VID = 104 (Leaf).
4. On NNI ingress, pop one tag
5. Match on an NNI (port 4) for root VID = 103 or leaf VID = 104, and inner VID=73.
6. Create a root up-MEP of instance 5, EVC flow 6, and service level 7.
7. Create a Leaf up-MEP of instance 6, EVC flow 6, and service level 7.

Figure 14 • **E-Tree Configuration**



Creating EVC

1. Create EVC.

```
evc 6 vid 103 ivid 103 interface GigabitEthernet 1/1 leaf vid 104 ivid
104 interface GigabitEthernet 1/2 learning policer none
```

2. Create an ECE for UNI#1 (leaf UNI).

```
evc ece 1 interface GigabitEthernet 1/2 outer-tag match type tagged vid
73 evc 6 policer none cc 4
```

3. Create an ECE for UNI#2 (root UNI).

```
evc ece 2 interface GigabitEthernet 1/3 outer-tag match type tagged vid
73 evc 6 policer none cc 4
```

Creating Root Up-MEP

1. Enable the Up-MEP instance

```
mep 5 up domain evc flow 6 level 7 interface GigabitEthernet 1/3
```

2. Configure the MEG-ID.

```
(config)# mep 5 meg-id ICC000MEG0001 ieee name DOMAIN000
```

3. Configure the MEP-ID.

```
mep 5 mep-id 1
```

4. Configure a peer MEP.

```
mep 5 peer-mep-id 2
```

5. Enable continuity check.

```
mep 5 cc 4 fr1s
```

Creating Leaf Up-MEP

1. Enable the Up-MEP instance

```
mep 6 up domain evc flow 6 level 7 interface GigabitEthernet 1/2
```

2. Configure the MEG-ID.

```
mep 6 meg-id ICC000MEG0002 ieee name DOMAIN001
```

3. Configure the MEP-ID.

```
mep 6 mep-id 2
```

4. Configure a peer MEP.

```
mep 6 peer-mep-id 3
```

5. Enable continuity check.

```
mep 6 cc 4 fr1s
```

Run the following commands to verify the configuration.

```
(config)# do show running-config
[...]
mep 5 up domain evc flow 6 level 7 interface GigabitEthernet 1/3
mep 5 meg-id ICC000MEG0001 ieee name DOMAIN000
mep 5 peer-mep-id 2
mep 5 cc 4
mep 6 up domain evc flow 6 level 7 interface GigabitEthernet 1/2
mep 6 meg-id ICC000MEG0002 ieee name DOMAIN001
mep 6 mep-id 2
mep 6 peer-mep-id 3
mep 6 cc 4
[...]

(config)# do show mep detail

MEP state is:
Inst  cLevel  cMeg  cMep  cAis  cLck  cLoop  cConf  cDeg  cSsf  aBlk
aTsd  aTsf  Peer MEP  cLoc  cRdi  cPeriod  cPrio
   5   False  True False  False False False  False  False True  True
False True         2  False False  False   False
   6   False  True False  False False False  False  False True  True
False True         3  False False  False   False

MEP Basic Configuration is:
```

```
Inst  Mode  Voe  Direct  Port  Dom  Level   Format     Name       Meg
id      Mep id  Vid  Flow  Eps  MAC
  5  Mep  Root       1/3  Evc  7   IEEE String DOMAIN000 ICC000MEG0001
1      0     6    0   00-01-C1-00-AF-B3
  6  Mep  Leaf       1/2  Evc  7   IEEE String DOMAIN001 ICC000MEG0002
2      0     6    0   00-01-C1-00-AF-B2

(config)# do show mep cc detail
MEP CC Configuration is:
Inst Prio Rate Tlv
5 4 1s
```

Port Protection Configuration

Disable Loop Protection and Spanning Tree using CLI

Port protection is a linear protection according to G.8031.

The following configuration example shows how MEP is used for linear protection. For more information, see Port Protection with Service OAM.

Loop protection and spanning tree must be disabled for ELPS to work. Any previously created MEP must be deleted using command `no mep <inst>`.

1. Change to interface 4,5 sub-mode.

```
(config)# interface GigabitEthernet 1/4,5
```

2. Disable Loop Protection.

```
(config-if)# no loop-protect
```

3. Disable Spanning Tree.

```
(config)# no spanning-tree
(config-if)# exit
```

Configure Port Protected VLAN using CLI

Configure the VLAN to be port protected. For more information, see VLAN OAM Configuration.

1. Create VLAN 111.

```
(config)# vlan 111
```

2. Configure the VLAN aggregation port.

```
(config)# interface GigabitEthernet 1/1
(config-if)# switchport hybrid native vlan 111
(config-if)# switchport hybrid allowed vlan 111
(config-if)# switchport hybrid port-type c-port
(config-if)# switchport mode hybrid
(config-if)# exit
```

3. Configure the VLAN protection ports.

```
(config)# interface GigabitEthernet 1/4,5
(config-if)# switchport hybrid native vlan 4095
(config-if)# switchport hybrid allowed vlan 111
(config-if)# switchport hybrid port-type s-port
(config-if)# switchport mode hybrid
(config-if)# exit
```

Configure Port Protected EVC using CLI

Configure the EVC to be port protected. For more information, see VLAN OAM.

1. Configure the UNI port.

```
(config)# interface GigabitEthernet 1/3
(config-if)# switchport hybrid native vlan 4095
(config-if)# switchport forbidden vlan add 111
(config-if)# switchport hybrid port-type c-port
(config-if)# switchport mode hybrid
(config-if)# exit
```

2. Configure PCP and DEI mapping to one-to-one on UNI and the protection ports.

```
(config)# interface GigabitEthernet 1/1,3,4,5
(config-if)# qos trust tag
(config-if)# qos map tag-cos pcp 0 dei 0 cos 0 dpl 0
(config-if)# qos map tag-cos pcp 0 dei 1 cos 0 dpl 1
(config-if)# qos map tag-cos pcp 1 dei 0 cos 1 dpl 0
(config-if)# qos map tag-cos pcp 1 dei 1 cos 1 dpl 1
(config-if)# qos map cos-tag cos 0 dpl 0 pcp 0 dei 0
(config-if)# qos map cos-tag cos 0 dpl 1 pcp 0 dei 1
(config-if)# qos map cos-tag cos 1 dpl 0 pcp 1 dei 0
(config-if)# qos map cos-tag cos 1 dpl 1 pcp 1 dei 1
(config-if)# exit
```

3. Create the EVC.

```
(config)# evc 1 vid 222 ivid 222 interface GigabitEthernet 1/4,5
(config)# evc ece 1 interface GigabitEthernet 1/3 outer-tag add
          pcp-mode mapped pcp 4 cos 4
```

Create Down-MEP on Protecting Port using CLI

Create port down-MEP on working and protecting port. For more information, see Port OAM Configuration.

1. Configure Down-MEP on working port.

```
(config)# mep 1 down domain port level 0 interface GigabitEthernet 1/4
(config)# mep 1 meg-id ICC000MEG0001 itu
(config)# mep 1 mep-id 1
(config)# mep 1 voe
(config)# mep 1 peer-mep-id 2
(config)# mep 1 cc 0 fr300s
```

2. Configure Down-MEP on protecting port.

```
(config)# mep 2 down domain port level 0 interface GigabitEthernet 1/5
(config)# mep 2 meg-id ICC000MEG0001 itu
(config)# mep 2 mep-id 1
(config)# mep 2 voe
(config)# mep 2 peer-mep-id 2
(config)# mep 2 cc 0 fr300s
```

Create 1:1 port protection instance with revertive enabled. Port 4 is the working port and port 5 Configure Down-MEP on Protecting Port using CLI

1. Configure Down-MEP on protecting port.

```
(config)# mep 2 down domain port level 0 interface GigabitEthernet 1/5
(config)# mep 2 meg-id ICC000MEG0001 itu
(config)# mep 2 mep-id 1
(config)# mep 2 voe
(config)# mep 2 peer-mep-id 2
(config)# mep 2 cc 0 fr300s
```

Configure Port Protection with MEP Relation using CLI

1. Create the ELPS instance.

```
(config)# eps 1 domain port architecture 1for1 work-flow GigabitEthernet
1/4
          protect-flow GigabitEthernet 1/5
```

2. Configure the working MEP, Protecting MEP and APS MEP relations.

```
(config)# eps 1 mep-work 1 mep-protect 2 mep-aps 2
! Configure the WTR timer
(config)# eps 1 revertive 10s
```

3. Run the following commands to verify the configuration.

```
(config)# do show running-config
[...]
eps 1 domain port architecture 1for1 work-flow GigabitEthernet 1/4
      protect-flow GigabitEthernet 1/5
eps 1 mep-work 1 mep-protect 2 mep-aps 2
eps 1 revertive 10s
[...]
(config)# do show eps detail
EPS state is:
     Inst    State  Wstate   Pstate   TxAps r b   RxAps r b   FopPm
FopCm   FopNr   FopNoAps
        1     SfP     Sf       Sf      SFp 0 0     NR 0 0     False
False   False   False
EPS Configuration is:
     Inst   Dom   Archi   Wflow   Pflow   Wmep   Pmep   APSmep  Direct
Revert   Wtr  Hold   Aps
        1   Port  1for1    4       5       1      2       2     Bidir
True    w10s   0   True
```

Create Protected VLAN Down-MEP on Protected Port using CLI

Create a protected VLAN down-MEP on the protected port. For more information, see Configure VLAN Domain OAM Down-MEP using CLI.

1. Enable the VLAN Down-MEP instance.

```
(config)# mep 3 down domain vlan flow 111 level 0 interface
GigabitEthernet 1/4
(config)# mep 3 meg-id ICC000MEG0001 itu
(config)# mep 3 mep-id 1
(config)# mep 3 voe
(config)# mep 3 peer-mep-id 2
(config)# mep 3 cc 7 fr300s
```

Create Protected VLAN Up-MEP on UNI using CLI

Create protected EVC Up-MEP on the UNI. For more information, see EVC Domain OAM Up-MEP Configuration using CLI.

1. Enable the EVC Up-MEP instance.

```
(config)# mep 4 up domain evc flow 1 level 7 interface GigabitEthernet
1/3
(config)# mep 4 meg-id ICC000MEG0001 ieee name DOMAIN000
(config)# mep 4 mep-id 1
(config)# mep 4 peer-mep-id
(config)# mep 4 cc 4 fr300s
```

Ring Protection Configuration Examples

A ring protection is a VLAN protection according to G.8032.

Disable Loop Protection and Spanning Tree using CLI

The following configuration example, related to the Service OAM, shows how MEP is used for ring protection. For more information, see Ring Protection with Service OAM.

Loop protection and spanning tree must be disabled for ERPS to work.

1. Change to interface 4,5 sub-mode.

```
(config)# interface GigabitEthernet 1/4,5
```

2. Disable Loop Protection.

```
(config-if)# no loop-protect
```

3. Disable Spanning Tree.

```
(config)# no spanning-tree
```

Configure Ring Protection for VLAN using CLI

Configure the VLAN to be ring protected. For more information, see VLAN OAM Configuration.

1. Create VLAN 111.

```
(config)# vlan 111
```

2. Configure the VLAN aggregation port.

```
(config)# interface GigabitEthernet 1/1
(config-if)# switchport hybrid native vlan 111
(config-if)# switchport hybrid allowed vlan 111
(config-if)# switchport hybrid port-type c-port
(config-if)# switchport mode hybrid
(config-if)# exit
```

3. Configure the VLAN ring ports.

```
(config)# interface GigabitEthernet 1/4,5
(config-if)# switchport hybrid native vlan 4095
(config-if)# switchport hybrid allowed vlan 111
(config-if)# switchport hybrid port-type s-port
(config-if)# switchport mode hybrid
(config-if)# exit
```

Configure ERPS Control VLAN using CLI

Configure the ERPS control VLAN.

1. Create ERPS control VLAN 333.

```
(config)# vlan 333
```

2. Configure the ERPS control VLAN on the ring ports.

```
(config)# interface GigabitEthernet 1/4,5
(config-if)# switchport hybrid allowed vlan 333
(config-if)# switchport mode hybrid
```

Configure Ring Protection for EVC using CLI

Configure an EVC to be ring protected. For more information, see EVC OAM Configuration.

1. Configure the UNI port.

```
(config)# interface GigabitEthernet 1/3
```

```
(config-if)# switchport hybrid native vlan 4095
(config-if)# switchport forbidden vlan add 111
(config-if)# switchport hybrid port-type c-port
(config-if)# switchport mode hybrid
(config-if)# exit
```

2. Configure PCP and DEI mapping to one-to-one on UNI and the protection ports.

```
(config)# interface GigabitEthernet 1/1,3,4,5
(config-if)# qos trust tag
(config-if)# qos map tag-cos pcp 0 dei 0 cos 0 dpl 0
(config-if)# qos map tag-cos pcp 0 dei 1 cos 0 dpl 1
(config-if)# qos map tag-cos pcp 1 dei 0 cos 1 dpl 0
(config-if)# qos map tag-cos pcp 1 dei 1 cos 1 dpl 1
(config-if)# qos map cos-tag cos 0 dpl 0 pcp 0 dei 0
(config-if)# qos map cos-tag cos 0 dpl 1 pcp 0 dei 1
(config-if)# qos map cos-tag cos 1 dpl 0 pcp 1 dei 0
(config-if)# qos map cos-tag cos 1 dpl 1 pcp 1 dei 1
(config-if)# exit
```

3. Create the EVC.

```
(config)# evc 1 vid 222 ivid 222 interface GigabitEthernet 1/4,5
(config)# evc ece 1 interface GigabitEthernet 1/3 outer-tag add
          pcp-mode mapped pcp 4 cos 4
```

Create Port Down-MEP on Ring Link Port 0 and 1 using CLI

Create port down-MEP on ring link 0 and ring link 1 port. For more information, see Configure Port Domain OAM Down-MEP using CLI.

1. Configure Down-MEP on ring link 0 port.

```
(config)# mep 1 down domain port level 0 interface GigabitEthernet 1/4
(config)# mep 1 meg-id ICC000MEG0001 itu
(config)# mep 1 mep-id 1
(config)# mep 1 voe
(config)# mep 1 peer-mep-id 2
```

Configure Down-MEP on Ring Link Port 1 using CLI

1. Configure Down-MEP on ring link 1 port.

```
(config)# mep 2 down domain port level 0 interface GigabitEthernet 1/5
(config)# mep 2 meg-id ICC000MEG0001 itu
(config)# mep 2 mep-id 1
(config)# mep 2 voe
(config)# mep 2 peer-mep-id 2
(config)# mep 2 cc 0 fr300s
```

Create ERPS control VLAN Down-MEP on Ring Link 0 and 1 using CLI

Create ERPS control VLAN down-MEP on ring link 0 and ring link 1. For more information, see Configure VLAN Domain OAM Down-MEP using CLI.

1. Enable the control VLAN Down-MEP with enabled RAPS on ring link 0.

```
(config)# mep 3 down domain vlan flow 333 level 0 interface
GigabitEthernet 1/4
(config)# mep 3 aps 0 raps
```

2. Enable the control VLAN Down-MEP with enabled RAPS on ring link 1

```
(config)# mep 4 down domain vlan flow 333 level 0 interface
GigabitEthernet 1/5
(config)# mep 4 aps 0 raps
```

In this implementation, the ring link0 and link1 are ports. The ERPS ICLI command parameter for this is port0 and port1.

Create a major ring protection instance as RPL owner, protecting VLAN 111 and EVC 1. Ring link port0 is Port 1/4 and ring link port1 is Port 1/5.

Ring Protection with MEP Relation Configuration Example

Configure Ring Protected VLANS using CLI

1. Create the ERPS instance.

```
(config)# erps 1 major port0 interface GigabitEthernet 1/4
port1 interface GigabitEthernet 1/5
```

2. Configure the Port-0 and Port-1 SF/APS MEP relations.

```
(config)# erps 1 mep port0 sf 1 aps 3 port1 sf 2 aps 4
```

3. Configure the RPL port.

```
(config)# erps 1 rpl owner port0
```

4. Configure the protected VLAN’s.

```
(config)# erps 1 vlan 111,222
```

5. Run the following commands to verify the configuration.

```
(config)# do show running-config
[...]
erps 1 major port0 interface GigabitEthernet 1/4 port1 interface
GigabitEthernet 1/5
erps 1 mep port0 sf 1 aps 3 port1 sf 2 aps 4
erps 1 rpl owner port0
erps 1 vlan 111,222
[...]
(config)# do show erps detail
Grp#  Port 0         Port 1         RPL:Role   Port    Blocking
   1  Gi 1/4         Gi 1/5         Owner      Port 0  Blocked
    Protected VLANS:
       222   111
    Protection Group State             :Active
    Port 0 SF MEP                      :1
    Port 1 SF MEP                      :2
    Port 0 APS MEP                     :3
    Port 1 APS MEP                     :4
    WTR Timeout                        :1
    WTB Timeout                        :5500
    Hold-Off Timeout                   :0
    Guard Timeout                      :500
    Node Type                          :Major
    Reversion                          :Revertive
    Version                            :2
    ERPSv2 Administrative Command      :None
    FSM State                          :PROTECTED
    Port 0 Link Status                 :Link Down
    Port 1 Link Status                 :Link Down
    Port 0 Block Status                :BLOCKED
    Port 1 Block Status                :BLOCKED
    R-APS Transmission                  :SF BPR 0
    R-APS Port 0 Reception              :NONE
    R-APS Port 1 Reception              :NONE
    FOP Alarm                           :OFFEPS Configuration is:
```

Create Protected VLAN Up-MEP on VLAN Aggregation Port using CLI

Create protected VLAN up-MEP on the VLAN aggregation port. For more information, see Configure VLAN Domain OAM Up-MEP using CLI.

1. Enable the VLAN Up-MEP instance.

```
(config)# mep 5 up domain vlan flow 111 level 3 interface
GigabitEthernet 1/1
(config)# mep 5 meg-id ICC000MEG0001 itu
(config)# mep 5 mep-id 1
(config)# mep 5 voe
(config)# mep 5 peer-mep-id 2
(config)# mep 5 cc 7 fr300s
```

Create Protected EVC Up-MEP on VLAN Aggregation Port using CLI

Create protected EVC up-MEP on the UNI port. For more information, see EVC Domain OAM Up-MEP Configuration using CLI.

1. Enable the EVC Up-MEP instance

```
(config)# mep 6 up domain evc flow 1 level 7 interface GigabitEthernet
1/3
(config)# mep 6 meg-id ICC000MEG0001 ieee name DOMAIN000
(config)# mep 6 mep-id 1
(config)# mep 6 voe
(config)# mep 6 peer-mep-id 2
(config)# mep 6 cc 4 fr1s
```

Ring Interconnection Protection Configuration

A ring interconnected protection is a VLAN protection according to G.8032.

Configure Ring Protected VLAN Instance using CLI

The following configuration example builds on the configuration in Ring Protection except that the major ring instance must be created slightly different. it also shows how MEP is used for interconnected ring protection. For more information, see Ring Interconnection Protection.

Create a major ring protection instance as interconnected and protecting sub-ring control VLAN.

1. Create the ERPS instance.

```
(config)# erps 1 major port0 interface GigabitEthernet 1/4
          port1 interface GigabitEthernet 1/5 interconnect
```

2. Configure the Port-0 and Port-1 SF/APS MEP relations.

```
(config)# erps 1 mep port0 sf 1 aps 3 port1 sf 2 aps 4
```

3. Configure the RPL port.

```
(config)# erps 1 rpl owner port0
```

4. Configure the protected VLAN’s including sub-ring control VLAN 444.

```
(config)# erps 1 vlan 111,222,444
```

Create Port Down-MEP on Sub-ring Link Port using CLI

Create a port down-MEP on sub-ring link port. For more information, see Configure Port Domain OAM Down-MEP using CLI.

1. Configure Down-MEP on sub-ring link port.

```
(config)# mep 7 down domain port level 0 interface GigabitEthernet 1/2
(config)# mep 7 meg-id ICC000MEG0001 itu
(config)# mep 7 mep-id 1
(config)# mep 7 voe
(config)# mep 7 peer-mep-id 2
(config)# mep 7 cc 0 fr300s
```

Create Sub-ring Control VLAN using CLI

Create a sub-ring control VLAN based on the configuration in Ring Protection.

1. Create VLAN 444.

```
(config)# vlan 444
```

2. Configure the VLAN sub-ring link port.

```
(config)# interface GigabitEthernet 1/2
(config-if)# switchport hybrid allowed vlan 444
(config-if)# switchport hybrid port-type s-port
(config-if)# switchport mode hybrid
(config-if)# exit
```

3. Configure the VLAN ring ports.

```
(config)# interface GigabitEthernet 1/4,5
(config-if)# switchport hybrid allowed vlan 111,333,444
(config-if)# switchport hybrid port-type s-port
(config-if)# switchport mode hybrid
(config-if)# exit
```

Create Sub-ring Control VLAN Down-MEP and Up-MEP using CLI

Create a sub-ring control VLAN down-MEP and up-MEP (virtual channel) on sub-ring link port.

1. Enable the VLAN Down-MEP instance on sub-ring link port.

```
(config)# mep 8 down domain vlan flow 444 level 0 interface
GigabitEthernet 1/2
(config)# mep 8 aps 0 raps
```

Enable VLAN Up-MEP Instance on Sub-Ring Virtual Channel using CLI

1. Enable the VLAN Up-MEP instance on sub-ring virtual channel.

```
(config)# mep 9 up domain vlan flow 444 level 0 interface
GigabitEthernet 1/2
(config)# mep 9 aps 0 raps
```

Configure Ring Interconnected Protection with MEP Relation using CLI

1. Create the ERPS sub-ring instance.

```
(config)# erps 2 sub port0 interface GigabitEthernet 1/2 interconnect 1
virtual-channel
```

2. Configure the Port-0 and virtual Port-1 SF/APS MEP relations.

```
(config)# erps 2 mep port0 sf 7 aps 8 port1 aps 9
```

3. Run the following commands to verify the configuration.

```
(config)# do show running-config
[...]
erps 1 major port0 interface GigabitEthernet 1/4 port1 interface
GigabitEthernet 1/5 interconnect
erps 1 mep port0 sf 1 aps 3 port1 sf 2 aps 4
erps 1 rpl owner port0
erps 1 vlan 111,222,444
erps 2 sub port0 interface GigabitEthernet 1/2 interconnect 1
virtual-channel
erps 2 mep port0 sf 7 aps 8 port1 aps 9
[...]
(config)# do show erps detail
Grp#  Port 0         Port 1         RPL:Role   Port    Blocking
   1  Gi 1/4         Gi 1/5         Owner      Port 0  Blocked
    Protected VLANS:
       111   222
    Protection Group State             :Active
    Port 0 SF MEP                      :1
    Port 1 SF MEP                      :2
    Port 0 APS MEP                     :3
    Port 1 APS MEP                     :4
    WTR Timeout                        :1
    WTB Timeout                        :5500
    Hold-Off Timeout                   :0
    Guard Timeout                      :500
    Node Type                          :Major-Interconnected
    Reversion                          :Revertive
    Version                            :2
    ERPSv2 Administrative Command      :None
    FSM State                          :PROTECTED
    Port 0 Link Status                 :Link Down
    Port 1 Link Status                 :Link Down
    Port 0 Block Status                :BLOCKED
    Port 1 Block Status                :BLOCKED
    R-APS Transmission                 :SF BPR 0
    R-APS Port 0 Reception             :NONE
    R-APS Port 1 Reception             :NONE
    FOP Alarm                          :OFF
Grp#  Port 0         Port 1         RPL:Role   Port    Blocking
   2  Gi 1/2         -              -          -       -
    Protected VLANS:
      None
    Protection Group State             :Active
    Port 0 SF MEP                      :7
    Port 1 SF MEP                      :0
    Port 0 APS MEP                     :8
    Port 1 APS MEP                     :9
    WTR Timeout                        :1
    WTB Timeout                        :5500
    Hold-Off Timeout                   :0
    Guard Timeout                      :500
    Node Type                          :Sub-Interconnected
    Major Ring ID                      :1
    Topology change propagation        :Disabled
    Virtual Channel                    :Yes
    Reversion                          :Revertive
    Version                            :2
```

```
ERPSv2 Administrative Command      :None
FSM State                          :PROTECTED
Port 0 Link Status                 :Link Down
Port 1 Link Status                 :Link Down
Port 0 Block Status                :BLOCKED
Port 1 Block Status                :BLOCKED
R-APS Transmission                 :SF DNF BPR 0
R-APS Port 0 Reception             :NONE
R-APS Port 1 Reception             :NONE
FOP Alarm                          :OFF
```

CHAPTER 9

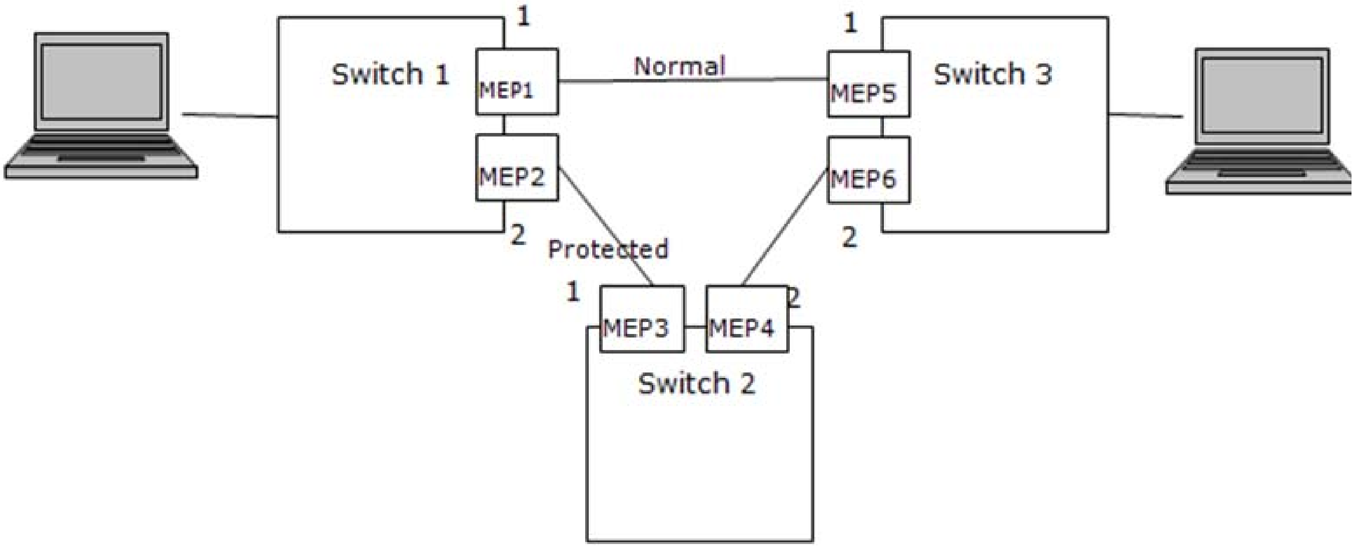
Ethernet Ring Protection Switching Configuration

Introduction

This document shows how to configure the Ethernet Ring Protection Switching (ERPS) for switches using the ICLI commands. The following figure shows the simple three switch network constructed to demonstrate these features.

Figure 9-1 Ethernet Ring Protection Switching (ERPS) Model

f



Configuring ERPS from the ICLI

Initial Switch Configuration

The following commands disable STP and LLDP, and they enable C-Port on Port 1 and 2 on all switches.

```
#Configure port 1-2
interface GigabitEthernet 1/1-2
 #set C-Port
 switchport hybrid port-type c-port
 switchport mode hybrid
 #disable LLDP
 no lldp receive
 no lldp transmit
 #disable Spanning Tree Protocol
 no spanning-tree
```

Configuring MEP and ERPS on Switch 1 (RPL Owner)

```
#create mep 1 on port 1
mep 1 down domain port flow 1 level 0 interface GigabitEthernet 1/1
#set vlan for MEP traffic
mep 1 vid 3001
#set id of peer mep
mep 1 peer-mep-id 5
#enable ccm, default is 1FPS
mep 1 cc 0
#enable RAPS
mep 1 aps 0 raps
mep 2 down domain port flow 2 level 0 interface GigabitEthernet 1/2
mep 2 mep-id 2
mep 2 vid 3001
mep 2 peer-mep-id 3
mep 2 cc 0
mep 2 aps 0 raps
#create erps on port 1 and port 2
erps 1 major port0 interface GigabitEthernet 1/1 port1 interface GigabitEthernet
1/2
#set MEP ID for the corresponding port
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
#set to RPL owner
erps 1 rpl owner port1\
#set protected VLAN
erps 1 vlan 1
```

Configuring MEP and ERPS on Switch 2 (RPL Neighbor)

```
mep 1 down domain port flow 1 level 0 interface GigabitEthernet 1/1
mep 1 mep-id 3
mep 1 vid 3001
mep 1 peer-mep-id 2
mep 1 cc 0
mep 1 aps 0 raps
mep 2 down domain port flow 2 level 0 interface GigabitEthernet 1/2
mep 2 mep-id 4
mep 2 vid 3001
mep 2 peer-mep-id 6
mep 2 cc 0
mep 2 aps 0 raps
erps 1 major port0 interface GigabitEthernet 1/1 port1 interface GigabitEthernet
1/2
```

```
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
#set to RPL neighbour
erps 1 rpl neighbor port0
erps 1 vlan 1
```

Configuring MEP and ERPS on Switch 3

```
mep 1 down domain port flow 1 level 0 interface GigabitEthernet 1/1
mep 1 mep-id 5
mep 1 vid 3001
mep 1 peer-mep-id 1
mep 1 cc 0
mep 1 aps 0 raps
mep 2 down domain port flow 2 level 0 interface GigabitEthernet 1/2
mep 2 mep-id 6
mep 2 vid 3001
mep 2 peer-mep-id 4
mep 2 cc 0
mep 2 aps 0 raps
erps 1 major port0 interface GigabitEthernet 1/1 port1 interface GigabitEthernet
1/2
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
erps 1 vlan 1
```

Note: On ME1200. To set the CCM rate to 100FPS or 300FPS, the peer MAC address must be known as shown here, Or set it to lower rate first, until the peer MAC address is learned, and then change it to a higher rate.

```
mep 1 peer-mep-id <peer mep id> mac <peer mac address>
mep 1 cc 0 fr300s
```

Finally, the ERPS status can be checked with the `show erps` command.

CHAPTER 10

Performance Monitor Configuration

Performance Monitoring (PM) is a Carrier Ethernet software feature that collects, stores, and transfers statistics from the Operations, Administration and Management (OAM) engine according to a user's configuration. These statistics relate to delay, loss, Ethernet Virtual Connections (EVC), EVC Control Entry (ECE), and more. The user can select which data to collect as well as the intervals for collection and transfer.

This document provides examples of how to setup the Performance Monitor feature with ME1200 Industrial Command Line Interface (ICLI). It also includes the command set and their meanings.

Configuration Options

This section describes the available configuration options.

Session, Storage, and Transfer Configuration

Up-MEP support is required for configuring the performance monitors.

Click **Configuration** > **Performance Monitor** to display the two choices, Configuration and Transfer Mode.

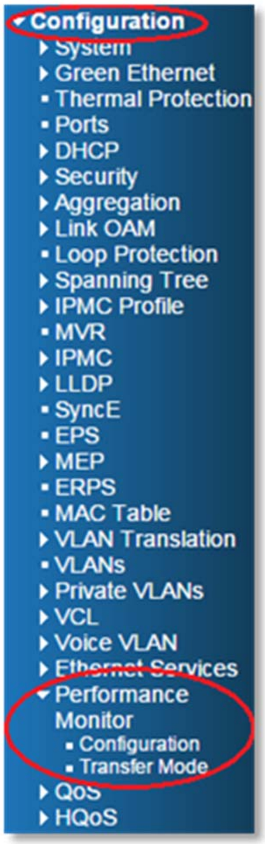
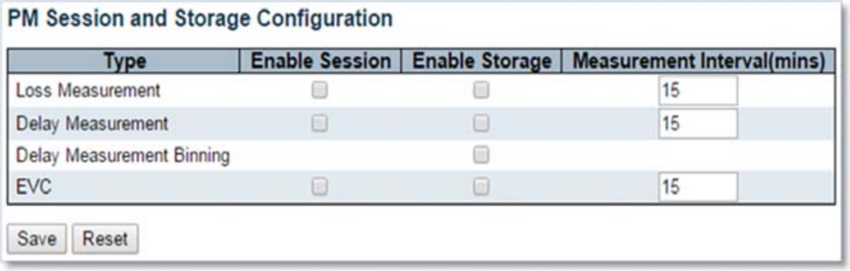


Figure 1 **• Performance Monitor Mode Configuration**

The following illustration shows the Configuration > Performance Monitor > Configuration options.



PM Session and Storage Configuration

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

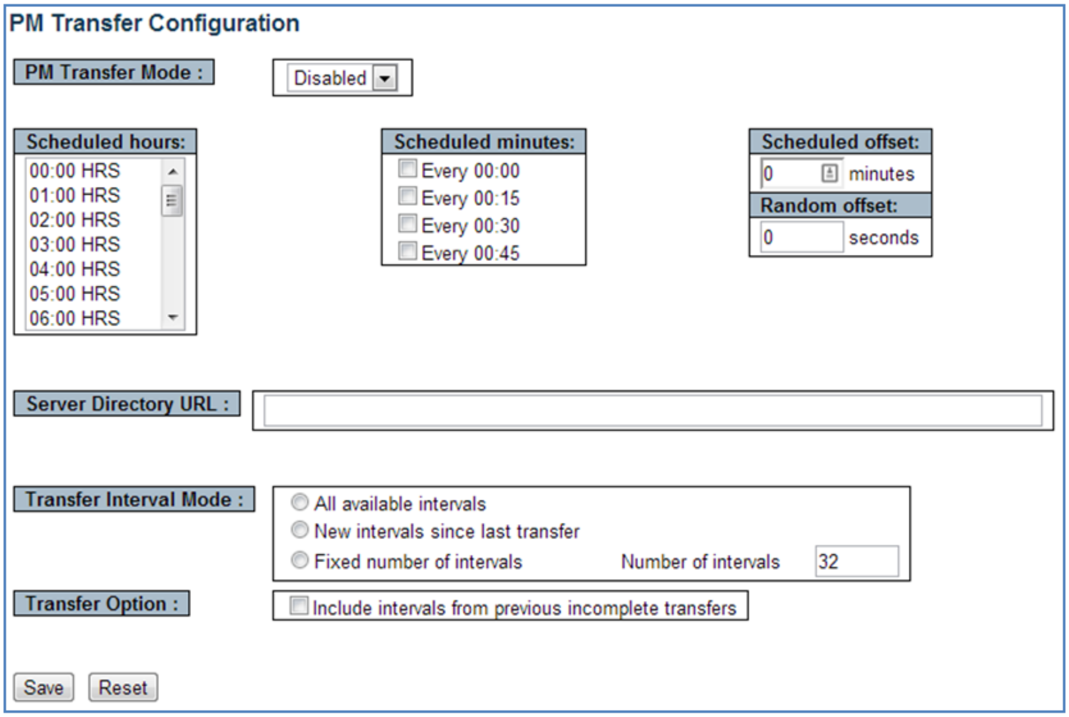
Figure 2 **• Session and Storage Configuration Options**

Session and storage configuration options are disabled by default. click the desired option to enable it. The following table lists the session and storage options.

Table 1 • **Sessions and Storage Options**

Term	Description
Type	The data type of performance monitor.
Enable Session	Enable or disable the performance monitor session.
Enable Storage	Enable or disable he performance monitor storage.
Measurement Interval	The measurement interval for the performance monitor.

The following illustration shows the Configuration > Performance Monitor > Transfer Mode options.



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

Figure 3 • **Transfer Configuration Options**

Transfer configuration options are disabled by default. To enable, choose Enabled with the desired settings and click Save. The following table lists the transfer configuration options.

Table 2 • **Transfer Configuration Options**

Term	Description
PM Transfer Mode	Configure the operation mode per system. Options are not available for a disabled mode.
Scheduled Hours	Select one or more scheduled hours when the PM data transfer will occur. The default is none selected. Multiple selections are supported.
Scheduled Minutes	Select one or more scheduled minutes when the PM data transfer will occur. The default is none selected. Multiple selections are supported.
Measurement Interval	The measurement interval for the performance monitor.

Table 2 • **Transfer Configuration Options (continued)**

Term	Description
Scheduled Offset	Specify a fixed offset to be added to the scheduled transfer time. The default is 0 minutes. The range is between 0 and 15 minutes. *Note: The sum of scheduled fixed offset and scheduled random offset must not exceed 15 minutes.*
Random Offset	Specify a random offset to be added to the scheduled transfer time. The default is 0 seconds. The range is between 0 to 900 seconds. The offset added to the scheduled transfer time is a random value in the range of 0 seconds to random offset. *Note: The sum of scheduled fixed offset and scheduled random offset must not exceed 15 minutes.*
Server Directory URL	The full URL of the server and the corresponding directory (if set properly) for uploading. HTTP and TFTP are supported. To enable HTTP, use http://<domain name or IP address> To enable TFTP, use tftp://<domain name or IP address>
Transfer Interval Mode	Supported interval modes: • All available intervals: To enable transfer of all completed measurement Intervals. • New intervals since last transfer: To enable transfer of only completed measurement Intervals since last transfer. • Fixed number of intervals: To enable transfer of all completed measurement Intervals up to the configured number.
Number of intervals	Specify the number of intervals to send when fixed number of interval is selected. The range is between 1 and 96 Intervals.
Transfer Option	Select this option to include intervals from previous incomplete transfers.

Statistics Reporting

Click **Monitor** > **Performance Monitor** to display the available choices.

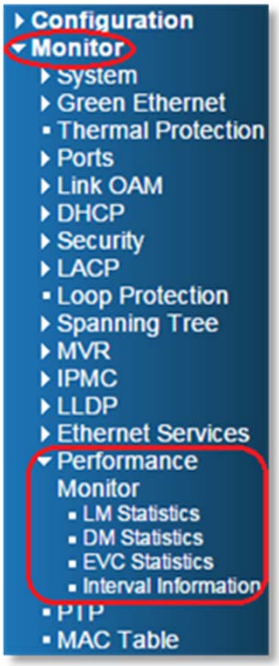
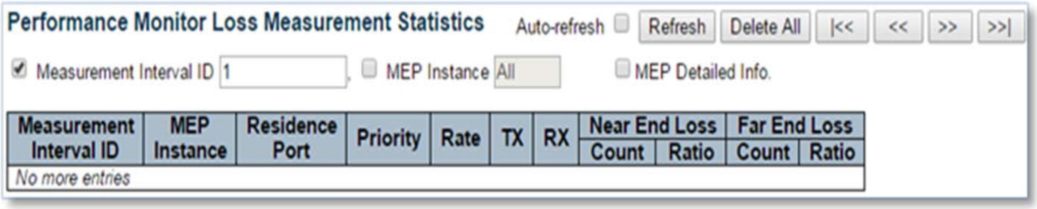


Figure 4 • **Performance Monitor Statistics Options**

The available choices are as follows:

- LM Statistics
- DM Statistics
- EVC Statistics
- Interval Information

The following illustrations show the options available for each of the four statistics options.

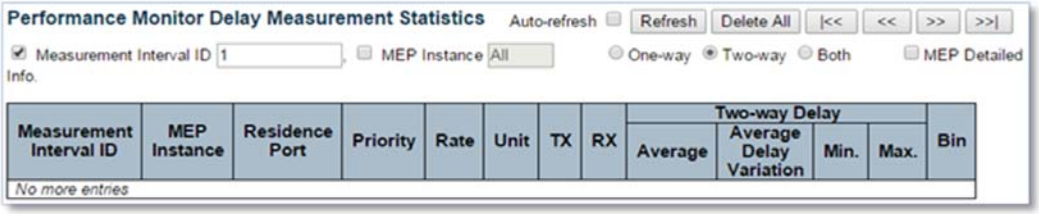


Performance Monitor Loss Measurement Statistics Auto-refresh □ Refresh Delete All |<< << >> >>|

☑ 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										

Figure 5 • **Loss Measurement Statistics**

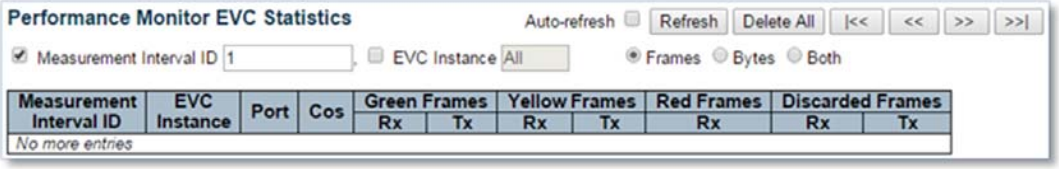


Performance Monitor Delay Measurement Statistics

☑ 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												

Figure 6 **• Delay Measurement Statistics**

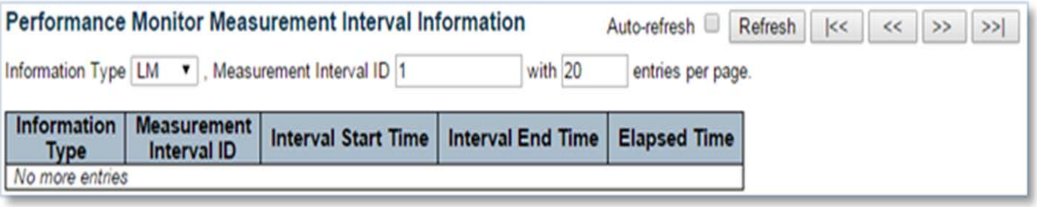


Performance Monitor EVC Statistics

☑ 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										

Figure 7 **• EVC Statistics**



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				

Figure 8 **• Measurement Interval Information**

Note: All measurement intervals are displayed if a measurement interval ID is not selected. The volume of measurement data to be displayed can make this a very time consuming process.

ICLI Show Commands

Show commands are available under exec mode. Outside of the exec mode, the commands may be invoked by the `do show <show commands>` command.

Show perf-mon current feature

Use the following syntax to display the current performance monitor measurement data for a specified feature.

```
show perf-mon current feature { dm | lm | evc }
```

In the following example, 237 is the current Interval ID.

```
# show perf-mon current feature evc Interval ID : 237
--------------------------------------------------------
   EVC instance = 10
   EVC port= 1
   Valid= yes
   Tx green frames= 1002
   Tx green bytes= 153602
   Tx yellow frames= 0
   Tx yellow bytes= 0
   Tx red frames= 0
   Tx red bytes= 0
   Tx discard frames = 0
   Tx discard bytes= 0
   Rx green frames= 930
   Rx green bytes= 142590
   Rx yellow frames= 0
   Rx yellow bytes= 0
   Rx red frames= 0
   Rx red bytes      = 0
   Rx discard frames = 0
   Rx discard bytes  = 0
```

Show perf-mon interval-id ID feature

Use the following syntax to display the specified current performance monitor measurement data for a specific interval and feature.

```
show perf-mon interval-id ID feature { dm | lm | evc }
```

where ID is the integer value of the specified interval. For example, if 144 is the interval ID to be queried, it can be used as follows:

```
# show perf-mon interval-id 144 feature evc Interval ID : 144
--------------------------------------------------------
   EVC instance = 10
   EVC port= 1
   Valid= yes
   Tx green frames= 832
   Tx green bytes= 831020
   Tx yellow frames= 0
   Tx yellow bytes= 0
   Tx red frames= 0
   Tx red bytes= 0
   Tx discard frames = 0
   Tx discard bytes= 0
   Rx green frames= 533
   Rx green bytes= 501324
   Rx yellow frames= 0
   Rx yellow bytes= 0
   Rx red frames= 0
   Rx red bytes      = 0
   Rx discard frames = 0
   Rx discard bytes  = 0
```

Show perf-mon interval-info feature

Use the following syntax to show the list of performance monitor intervals of a specific feature.

```
show perf-mon interval-info feature { dm | lm | evc }
```

When querying past measurement information a measurement ID needs to be queried first, as shown in the following example.

```
# show perf-mon interval-info feature eve EVC Interval Information
--------------------------------------------------------
Measurement interval ID = 143
Start time= 1970-01-01T02:01:25+00:00
End time= 1970-01-01T02:02:25+00:00
End time= 60 seconds Measurement interval ID = 144
Start time= 1970-01-01T02:02:25+00:00
End time= 1970-01-01T02:03:25+00:00
End time= 60 seconds Measurement interval ID = 145
```

```
Start time= 1970-01-01T02:03:25+00:00
End time= 1970-01-01T02:04:25+00:00
End time= 60 seconds
…
```

ICLI Configuration Commands

Configuration commands are available under the global configuration mode, which is invoked by the `configure terminal` or `conf t` command. To exit global configure mode, type `end`.

```
# conf t
(config)# perf-mon ?
interval Measurement interval
session Session Enabled
storage Storage Enabled
transfer Transfer Mode Enabled
(config)# end
```

The following table shows the available commands and their usage.

Table 3 • **Commands and Usage**

Command	Usage
`perf-mon interval`	Set the measurement interval use. `perf-mon interval { dm | lm | evc } interval` where interval is an integer value within the range of 1 to 60 minutes.

`perf-mon session`	Enable the performance monitor session for the feature(s) specified.
	`perf-mon session { dm | lm | evc }`
	Disable the performance monitor session for the feature(s) specified.
	`no perf-mon session { dm | lm | evc }`

Table 3 • **Commands and Usage (continued)**

Command	Usage

`perf-mon transfer`	Configure the method and time used to handle the performance monitor data. When transfer is disabled, all transfer sub-commands are ineffective.
	Enable the transfer of measurement data to the specified remote server.
	`perf-mon transfer`
	Disable the transfer of measurement data.
	`no perf-mon transfer`

	Specify the destination for the measurement data upload.
	`perf-mon transfer url URL`
	where URL can be in the following form.
	tftp://<ip address>/
	http://<domain name>/
	tftp://<ip address>/
	http://<domain name>/
	Clear the transfer URL
	`no perf-mon transfer url`

	Set the transfer mode. `perf-mon transfer mode { all | fixed | new }` where: `All`: All available intervals (default when none are specified) `Fixed`: Fixed number of intervals `New`: New intervals since last transfer

Table 3 • **Commands and Usage (continued)**

Command	Usage

	Enable the inclusion of previous incomplete transfers with the current interval transfer.
	`perf-mon transfer incomplete`
	Disable the inclusion of previous incomplete transfers with the current interval transfer.
	`no perf-mon transfer incomplete`

	Specify a transfer time. This command can be specified multiple times to specify the different hours of a day. Transfer time is comprised of the following commands.
	`perf-mon transfer hour <0-23>`
	`perf-mon transfer minute { 0 | 15 | 30 | 45 }`
	`perf-mon transfer fixed-offset <0-15>`
	`perf-mon transfer random-offset <0-900>`
	The minute command can be specified multiple times to specify the different minutes of an hour. If data is to be transferred four times per hour, set all of them. The fixed-offset is a single offset setting that is added to transfer hour and minute to allow a range between 0 and 15 minutes.
	The random time offset is added to the previous time configurations and accepts a value between 0 and 900 seconds. This is useful when all switches are time synchronized and configuration is copied across all switches. This avoids all switches uploading data at the same moment, which may overload the TFTP or HTTP server.
	Each of the transfer time commands support a negate feature.
	`no perf-mon transfer hour`
	`no perf-mon transfer hour x`
	`no perf-mon transfer minute`
	`no perf-mon transfer minute x`
	`no perf-mon transfer fixed-offset`
	`no perf-mon transfer random-offset`
	Commands with parameters remove the indicated parameter only. If no parameter is provided, all settings for the command are removed.

Configuration Example

The following Performance Monitor configuration example is shown in both ICLI and GUI form. The configuration is displayed by executing `show running-config`.

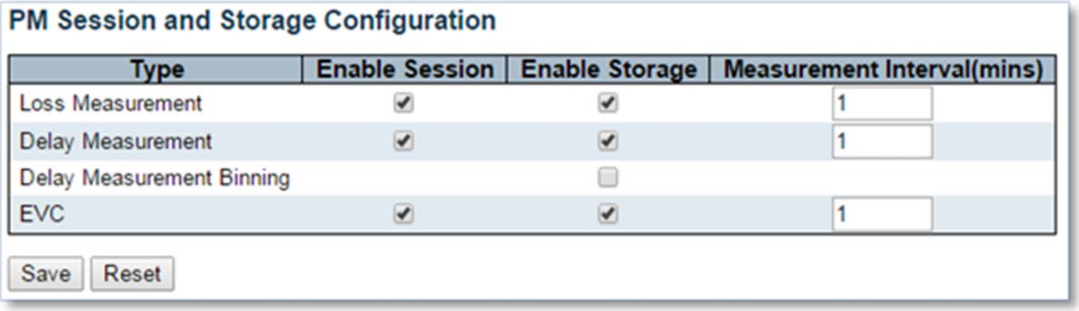
```
username admin privilege
15 password none
evc 10 vid 1000 ivid 1000
interface GigabitEthernet 1/3
evc ece 1 interface
GigabitEthernet 1/1 outer-tag match type tagged pcp 4-7 add pcp-mode mapped
dei-mode dp evc 10 cos 4
evc ece 2 interface
GigabitEthernet 1/1 outer-tag add pcp-mode mapped dei-mode dp rule-type rx evc
10 cos 0
!
vlan 1
 name default
```

```
!
!
!
spanning-tree mst name
00-01-c1-00-af-d0c2-30 revision 0

upnp
access-list ace 1 policy
42 tag-priority 0 frametypeframe-type etype dmac 01-80-c2-00-00-0e action deny
network-clock
wait-to-restore 5
voice vlan oui 00-01-E3 description Siemens AG
phones
voice vlan oui 00-03-6B description Cisco phones
voice vlan oui 00-0F-E2 description H3C phones
voice vlan oui 00-60-B9 description Philips and NEC
AG phones
voice vlan oui 00-D0-1E description Pingtel phones
voice vlan oui 00-E0-75 description Polycom phones
voice vlan oui 00-E0-BB description 3Com phones
perf-mon session lm
perf-mon session dm
perf-mon session evc
perf-mon session ece
perf-mon storage lm
perf-mon storage dm
perf-mon storage evc
perf-mon storage ece
perf-mon interval lm 1
perf-mon interval dm 1
perf-mon interval evc 1
perf-mon interval ece
1
perf-mon transfer
perf-mon transfer hour 0
perf-mon transfer hour 3
perf-mon transfer hour 6
perf-mon transfer hour 9
perf-mon transfer hour 12
perf-mon transfer hour 15
perf-mon transfer hour 18
perf-mon transfer hour 21
perf-mon transfer minute 0
perf-mon transfer minute
15
perf-mon transfer minute
30
perf-mon transfer minute
45
perf-mon transfer
fixed-offset 1
perf-mon transfer url
tftp://10.1.0.60/
perf-mon transfer mode all
perf-mon transfer
incomplete
!
interface GigabitEthernet
1/1
```

```
 switchport hybrid native vlan 4095
 switchport hybrid allowed vlan none
 switchport mode hybrid
 link-oam
 link-oam link-monitor supported
!
interface GigabitEthernet
1/2
!
interface GigabitEthernet
1/3
 switchport hybrid native vlan 4095
 switchport hybrid allowed vlan none
 switchport hybrid port-type s-port
 switchport mode hybrid
 link-oam
 link-oam mode active
 link-oam link-monitor supported
!
interface GigabitEthernet
1/4
!
interface GigabitEthernet
1/5
!
interface GigabitEthernet
1/6
!
interface GigabitEthernet
1/7
!
interface GigabitEthernet
1/8
!
interface GigabitEthernet
1/9
!
interface
GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
interface vlan 1
 ip address dhcp
!
mpls tp
 global-id 0
 router-id
0.0.0.0
 icc-carrier-code NONE
!
mep os-tlv oui 0xC sub-type 0x1 value 0x2
mep 1 down domain port
flow 1 level 0 interface GigabitEthernet 1/1
mep 1 voe
mep 1 peer-mep-id 2
mep 1
performance-monitoring
mep 1 cc 0
mep 3 down domain port flow
3 level 0 interface GigabitEthernet 1/3
mep 3 voe
mep 3 peer-mep-id 2
mep 3
performance-monitoring
mep 3 cc 0
mep 10 down domain evc
flow 10 level 1 interface GigabitEthernet 1/3
mep 10 voe
mep 10 peer-mep-id 2
mep 10
performance-monitoring
mep 10 cc 4
mep 20 up domain evc
flow 10 level 2 interface GigabitEthernet 1/1
mep 20 voe
mep 20 peer-mep-id 2
mep 20
performance-monitoring
mep 20 cc 0
eps 1 domain port
architecture 1plus1 work-flow GigabitEthernet 1/1 protect-flow GigabitEthernet
1/2
eps 1 mep-work 3
mep-protect 1 mep-aps 1
eps 1 1plus1
unidirectional
!
spanning-tree aggregation
 spanning-tree link-type point-to-point
!
!
line console 0
 exec-timeout 0 0
 length 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
```

```
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
!
line vty 15
!
end
```

The following illustration shows the session and storage configuration in the GUI.

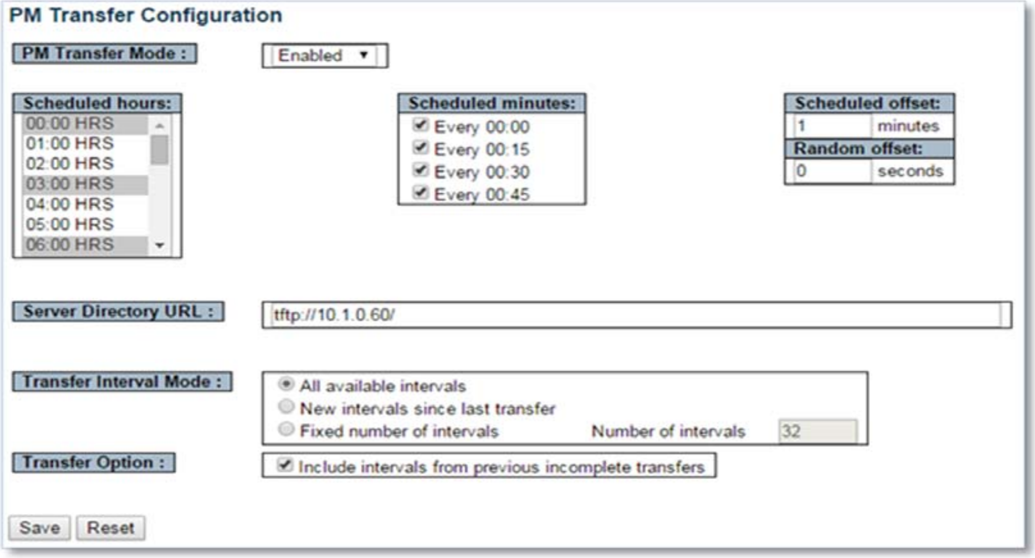


PM Session and Storage Configuration

Type	Enable Session	Enable Storage	Measurement Interval(mins)
Loss Measurement	☑	☑	1
Delay Measurement	☑	☑	1
Delay Measurement Binning		□	
EVC	☑	☑	1

Figure 9 **• PM Session and Storage Configuration**

The following illustration shows the transfer configuration in the GUI.



PM Transfer Configuration

PM Transfer Mode : Enabled

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: 1 minutes

Random offset: 0 seconds

Server Directory URL : tftp://10.1.0.60/

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

Figure 10 **• PM Transfer Configuration**

CHAPTER 11

Configuring the Network Access Server and Access Control List

This document describes how to configure Network Access Server (NAS) and Access Control List (ACL) functionality within the Switch Application Software of Cisco ME1200. Configuration can be performed through the web GUI or by means of the Industrial Command Line Interface (ICLI).

In the web GUI, NAS is found under Configuration > Security > Network > NAS. ACL is found under Configuration > Security > Network > ACL.

Access Control List

The access control list (ACL) is controlled with the ICLI command access-list in the config- and interface config mode. For more information about config and interface config modes, see Understanding Modes and Sub-Modes. The basic configuration commands are as follows:

```
(config)# access-list …
```

and

```
(config-if)# access-list …
```

In the web GUI, configuration is accessed using the following menus:

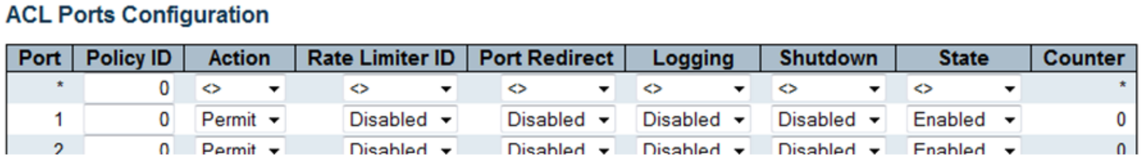
- **Configuration** > **Security** > **Network**> **ACL**
- **Configuration** > **Ethernet Services** > **EVCs**

The following sections describe the three ACL configuration categories: Ports, Rate Limiters, and Access Control List.

Ports

For each port, a rule can be configured for what should happen with an ingress packet. For the rule on a port to take effect, the packet in question must be associated with a policy ID. For now, we will assume that the policy ID is 0. This is the value a packet is associated with if no effort has been made to change that. For information about the policy ID, see "ECE Configuration Policy ID" on page 3.

The following illustration shows the web GUI for ACL Ports Configuration with one rule for each port.



ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Logging	Shutdown	State	Counter
*	0	<>	<>	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0

Figure 1 • **Port ACL**

Action can be *Permit* or *Deny*. Permit means that packets received on that port are forwarded the normal way, whereas Deny means that packets are ejected. So if we set Action to Deny for port 1 with PolicyID=0, then no packets are switched through the system.

Rate Limiter ID can be *Disabled* or a number in the range of 1-16, which points to one of the 16 rate limiters instances. The rate limiter ID maps to a packets per second number, which defines the rate. For more information see "Rate Limiters" on page 2.

Port Redirect specifies that packets matching the rule in question are redirected to a given port, or if *Disabled* should be forwarded the normal way, in which case the port redirect is disabled.

Logging specifies that packets matching the rule are logged. The packets can be displayed by the following ICLI command

```
# show logging
```

This shows a log with one item per incident. Use the following command to display the full information for incident 46.

```
# show logging 46
```

Shutdown specifies that when the rule is hit, then the port shall be shutdown.

State specifies whether the port is enabled or disabled. Changing it to *Disable*, turns the port off. If *Shutdown* is enabled and the rule is hit, then the system will change the value to *Disable*. Re-enable the port by changing it to *Enable*. It will stay enabled until the next time the rule is hit.

Counter tells how many times this rule has been hit.

Use the following ICLI commands to set up these rules from the interface-config mode.

```
(config-if)# access-list policy <PolicyID>
(config-if)# access-list action <deny | permit>
(config-if)# access-list rate-limit <1-16>
(config-if)# access-list redirect interface gi 1/2
(config-if)# [no] access-list logging
(config-if)# [no] access-list shutdown
(config-if)# access-list port-state
```

This command cannot be used to give several parameters in one line. Logging and shutdown is disabled with the `no` command.

The last of the commands are not in the web GUI. They are used to enable a port that has been shut down from when shutdown was enabled.

Rate Limiters

Rate limiters map rate limiter IDs to a rate. The rate can be given in any of the following formats.

- Packets per second
- 100 pps (100 packets per second)
- 100 kbps (100 kilobits per second)

The rate limit ID is a number between 1 and 16.

The ICLI command for setting the rate limit can be one of the following:

```
(config)# access-list rate-limiter <1-16> pps <0-131071>
(config)# access-list rate-limiter <1-16> 100pps <0-32767>
```

```
(config)# access-list rate-limiter <1-16> 100kbps <0-10000>
```

where <1-16> represents the number 1 to 16. The rate is the last number times the unit.

Access Control List

In the Ports section above, a list of rules, one per port, along with associated actions were defined. In this section more complicated rules will be described.

In this example the selected source MAC address shall be 00-00-00-00-00-12 and the destination MAC shall be broadcast. Also the EtherType shall be 0x9876. The VLAN ID shall be 2 and priority 2 or 3. So if an ingress packet on any port (since the Ingress Port is set to All) has these attributes, then it will match this rule. Upon a match the actions mentioned will be performed.

The ICLI command for building this rule is as follows. For clarity each element is placed one a separate line, but can be written on a single line.

```
(config)# access-list ace 1
                      vid 2
                      tag-priority 2-3
                      dmac-type broadcast
                      frametype etype
                      etype-value 0x9876
                      smac 00-00-00-00-00-12
                      logging
```

This ACE entity has the number 1. This number is called the AceId, which can be in the range of 1-512.

```
(config)# access-list ace <AceId> …
```

The elements in the command can be in any order, except that ace <AceId> must come first.

When adding more than one rule, which likely will be the case, then the rules are parsed in some order. When a rule is added similar to the one above, it is put in the end of the list. So it will be the last rule to be checked, until another rule is added.

It is possible to specify where a rule shall be inserted in the hierarchy. This is done by specifying which rule shall come next. This is demonstrated as follows, assuming an empty ACL list.

```
(config)# access-list ace 20 vid 100
(config)# access-list ace 15 vid 101
(config)# access-list ace 25 vid 102 next 15
```

The first command will insert the aceID 20 into an empty list. It is the first and only element. The aceID 15 is then inserted at the end of the list to lead to the order 20, 15. The next 15 field in the third aceID inserts it before rule 15. The resulting rule order is 20, 25, 15.

ECE Configuration Policy ID

Policy ID was set to 0 in Ports (ignore), and any in Access Control List.

An ECE rule goes into the IS1, before the IS2 where the ACL rule resides. Therefore when the Policy ID in the Actions table is given some value for an ECE, that value can be used in ACLs.

The ICLI command is:

```
(config)# evc ece <EceId> policy <Policy ID> …
```

Network Access Server

Types of NAS

This feature provides access control on a port basis. There are two types of authentication, namely IEEE 802.1X and MAC based. The 802.1X provide the following three kinds:

- Port based 802.1X
- Single 802.1X
- Multi 802.1X

The following three terms are used in the 802.1X context:

- Supplicant, client (PC) with some 801.1X software
- Authenticator, the switch
- Authentication server, e.g. a RADIUS server

So the supplicant/client is connected to the authenticator/switch on some port, and the authenticator can reach an authentication server.

The idea is that the supplicant wants access to the port, so it sends an Extensible Authentication Protocol over LAN (EAPoL) message to the authenticator, which in turn asks the authenticator server, if this supplicant can be accepted. If so, then the authenticator opens the port for the supplicant, and communication can begin. Depending on how the authenticator is configured, this process behaves in different ways.

Port Based 801.1X

In this method if the supplicant, S, is on a network, N, which is connected to the authenticator on some port, A, then if S opens port A, then everyone on network N has access.

Single 802.1X

This mode is similar to port based 802.1X, however in this case only the supplicant that did open the port on the authenticator is allowed to transmit and receive packets. This is done by means of the supplicant MAC address.

Multi 802.1X

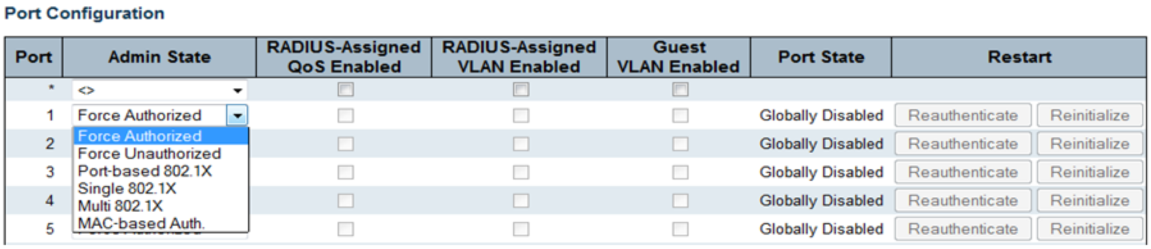
This mode is similar to single 802.1X, except here more than one supplicant can register on the port. One fine point here is that multicast packets are not sent to the supplicants from the switch.

MAC Based Authentication

If one thinks of a supplicant as consisting of a client and of a supplicant component that takes care of negotiating the port opening when the client transmits the first packet, then MAC based authentication can be understood as multi 802.1X where the supplicant component is moved into the authenticator/switch. This embedded supplicant component then uses the MAC address of the client as the user name and password in the form aa-bb-cc-dd-ee-ff. This has the advantage that the client does not have to have supplicant software.

Port Configuration

The following illustration shows the web interface with the six admin state options. The four of them are described above. The remaining two are Force Authorized and Force Unauthorized. The first is the default, which means the port is open. The second means that there is no access.



Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart
*	<>	□	□	□		
1	Force Authorized	□	□	□	Globally Disabled	Reauthenticate Reinitialize
2		□	□	□	Globally Disabled	Reauthenticate Reinitialize
3		□	□	□	Globally Disabled	Reauthenticate Reinitialize
4		□	□	□	Globally Disabled	Reauthenticate Reinitialize
5		□	□	□	Globally Disabled	Reauthenticate Reinitialize

Figure 2 • **NAS Port Configuration**

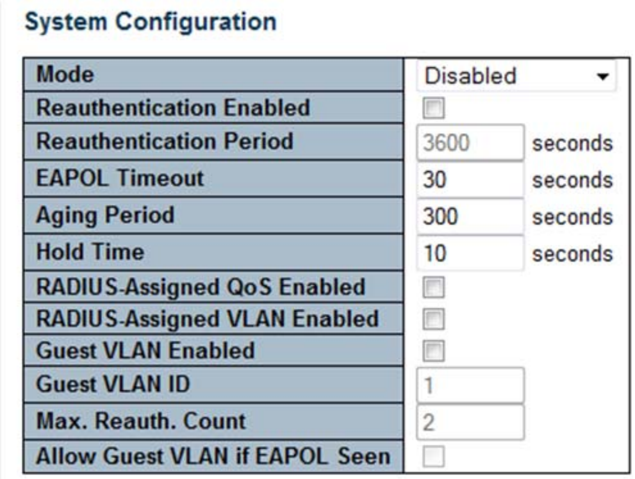
The ICLI commands for changing admin state options are as follows:

```
(config-if)# dot1x port-control auto |
                                force-authorized |
                                force-unauthorized |
                                mac-based |
                                multi |
                                single
```

Note: Auto means port based 802.1X as described in the following section.

System Configuration

After the admin state has been set for the ports, the NAS feature has to be enabled on the switch or authenticator. The following illustration shows the system configuration options.



System Configuration

Mode	Disabled
Reauthentication Enabled	□
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	□
RADIUS-Assigned VLAN Enabled	□
Guest VLAN Enabled	□
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	□

Figure 3 • **NAS System Configuration**

Mode

Mode enables the NAS functionality globally. The corresponding ICLI command is as follows.

```
(config)# [no] dot1x system-auth-control
```

Re-authentication Enabled

Re-authentication is enabled by the following ICLI command:

```
(config)# [no] dot1 re-authentication
```

The **no** variant disables it. This means that the supplicant is re-authenticated on a periodic basis. The period is the re-authentication period.

This parameter affects ports with port based 801.1X, single 802.1X, or multi 802.1X admin states.

If a supplicant does not re-authenticate, the authenticator releases the resources that were associated with it.

Note: For MAC based authentication, similar functionality is provided by the aging period.

Re-authentication Period

The re-authentication period is set by the following ICLI command:

```
(config)# [no] dot1x authentication timer re-authenticate <1-3600>
```

where <1-3600> is the time in seconds. The **no** variant sets it to the default, which is 3600 seconds.

This attribute is associated with re-authentication enabled attribute.

EAPOL Timeout

The EAPOL timeout is set by the following ICLI command:

```
(config)# [no] dot1x timeout tx-period <1-65535>
```

The **no** variant sets it to the default, which is 30 seconds.

This parameter affects ports with port based 801.1X, single 802.1X, or multi 802.1X admin states.

The EAPOL timeout is the re-transmission time for request identity EAPoL frames from the authenticator towards the supplicant.

Aging Period

The aging period is set by the following ICLI command:

```
(config)# [no] dot1x authentication timer inactivity <10-1000000>
```

The default is 300 seconds.

This parameter affects ports with single 801.1X, multi 802.1X, or MAC based authentication. In these cases, together with port based 802.1X, re-authentication handles the timeout, if enabled.

Aging is a kind of timeout for MAC based authentication. If a client has been registered by this method, and has not been heard from for greater than the aging period, then the authenticator releases the resources that were associated with it.

Hold Time

The hold time is set by the following ICLI command:

```
(config)# [no] dot1x timeout quite-period <10-1000000>
```

Where the **no** variant sets the hold time to the default, which is 10 seconds.

This parameter affects ports with single 801.1X, multi 802.1X, or MAC based authentication.

If a supplicant or client is denied access, it will be held in an unauthorized state for the hold time.

RADIUS

The RADIUS assigned QoS is globally enabled by the following ICLI command:

```
(config)# [no] dot1x feature radius-qos
```

The RADIUS assigned VLAN feature is enabled by the following ICLI command:

```
(config)# [no] dot1x feature radius-vlan
```

Both can be enabled by the following ICLI command:

```
(config)# [no] dot1x feature radius-qos radius-vlan
```

Guest VLAN

The guest vlan feature is enabled by the following ICLI command:

```
(config)# [no] dot1x feature guest-vlan
```

Any combination of the features guest-vlan, radius-qos, and radius-vlan can be enabled by the following ICLI command:

```
(config)# [no] dot1x feature guest-vlan radius-qos radius-vlan
```

RADIUS Assigned QoS

This feature is enabled for a port from the web interface. For more information, see "System Configuration" on page 5. It can also be enabled by the following ICLI command:

```
(config-if)# [no] dot1x radius-qos
```

where the **no** variant command disables it.

The feature takes effect when globally enabled by checking the RADIUS-Assigned QoS Enabled option, or by means of the following ICLI command:

```
(config)# [no] dot1x radius-qos
```

On the RADIUS server and entry (per RFC 4675), say:

```
User-Priority-Table = 55555555
```

must exist for the 802.1X entry in question. In this case the user is assigned QoS 5. Valid values are 0,…,7. The value on the right must contain eight identical numbers.

If the FreeRADIUS (http://freeradius.org) is used, then an entry for user mememe with password itsasecret would look like the following in the user's file.

```
mememe   Cleartext-password := “itsasecret”
         User-Priority-Table = 55555555
```

The port state table displays the admin state used, the port authorized, and the QoS class (5), as it was configured on the RADIUS server.

The **show dot1x** ICLI commands also display status and statistics.

```
# show dot1x status
# show dot1x status interface gi 1/3
The latter shows status to the interface specified:
# show dot1x status interface GigabitEthernet 1/3
GigabitEthernet 1/3 :
---------------------
Admin State         Port State             Last Source        Last ID
------------------  ---------------------  -----------------  -------
Port-based 802.1X   Authorized             00-23-5a-a8-05-eb  mememe
Current Radius QOS    Current Radius VLAN   Current Guest VLAN
--------------------  --------------------  --------------------
5                     -                     -
```

RADIUS Assigned VLAN

This feature is enabled for a port from the web interface. For more information, see "System Configuration" on page 5**.** It can also be enabled by the following ICLI command:

```
(config-if)# [no] dot1x radius-vlan
```

where the **no** variant disables it.

The feature takes effect when globally enabled by checking the RADIUS-Assigned VLAN Enabled option, or by means of the following ICLI command:

```
(config)# [no] dot1x radius-vlan
```

On the RADIUS server and entry, say:

```
Tunnel-Medium-Type = 6            i.e., IEEE-802
Tunnel-Type = 13                  i.e., VLAN
Tunnel-Private-Group-Id = ”123”   i.e., VID=123
```

must exist for the 802.1X entry in question. In this case, the user is assigned VLAN 123. Refer to RFC 2868, RADIUS Attributes for Tunnel Protocol Support and RFC 3580, IEEE 802.1X Remote Authentication Dial In User Service (RADIUS), Usage Guidelines for further reference.

If the FreeRADIUS (http://freeradius.org) is used, then an entry for user mememe with password itsasecret would look like the following in the user's file.

```
mememe   Cleartext-password := “itsasecret”
         User-Priority-Table = 55555555,
         Tunnel-Medium = 6,
         Tunnel-Type = 13,
         Tunnel-Private-Group-ID = 123
```

The QoS = 5 remains from the previous section.

The port state table shows that the port VLAN has been assigned by the RADIUS server.

The **show dot1x** ICLI command also shows the status information

```
# show dot1x status interface GigabitEthernet 1/3
GigabitEthernet 1/3 :
---------------------
Admin State          Port State              Last Source        Last ID
------------------   ---------------------   -----------------  -------
Port-based 802.1X    Authorized              00-23-5a-a8-05-eb  mememe

Current Radius QOS     Current Radius VLAN   Current Guest VLAN
--------------------   --------------------  --------------------
5                      123                   -
```

where VID 123 is found again.

Guest VLAN

A guest VLAN is a VLAN into which clients can be placed if the authentication process fails. This applies to cases where the admin state is single 801.1X, multi 802.1X, or MAC based authentication.

A port is enabled to enter the guest VLAN if the Guest VLAN Enabled option is selected in the web interface. For more information, see "System Configuration" on page 5. It can also be enabled by the following ICLI command:

```
(config-if)# [no] dot1x guest-vlan
```

Command parameters relate to the last four options in the web interface.

- Guest VLAN Enabled
- Guest VLAN ID
- Max. Reauth. Count
- Allow Guest VLAN if EAPoL Seen

The ICLI commands for these parameters are as follows:

```
(config)# [no] dot1x feature guest-vlan
(config)# dot1x guest-vlan 44
(config)# dot1x max-reauth-req 33
(config)# [no] dot1x guest-vlan supplicant
```

This command enables the guest vlan globally, sets the VLAN ID to 44, sets the Max. Reauth. Count to 33, and enables Allowed Guest VLAN if EAPOL See*n*.

The criteria for entering the guest VLAN is as follows:

After a link-up on a port, the authenticator starts transmitting EAPoL packets towards the supplicant. If Max. Reauth. Count packets are transmitted without receiving an EAPoL packet, then the port will enter the guest VLAN using the following logic:

- Allow Guest VLAN if EAPOL Seen is enabled

or

- Allow Guest VLAN if EAPOL Seen is not enabled:
  - If EAPoL packets have been seen on this port, then continue transmitting EAPoL packets and do not enter guest VLAN
  - If EAPoL packets have not been seen on this port, then enter guest VLAN.

CHAPTER 12

QoS Configuration

This document gives examples on how to set up Quality of Service (QoS) using the Industrial

Command Line Interface (ICLI) of Cisco ME1200. The examples used in this document pertain to ME1200 switch engine.

Understanding QoS

All incoming frames are classified to a QoS class, which is used in the queue system when assigning resources, in the arbitration from ingress to egress queues, and in the egress scheduler when selecting the next frame for transmission.

- Bandwidth control in the queues can be done by using Policers or Shapers.
- Apart from Shapers and Policers, different scheduling mechanisms can be configured on how the different priority queues in the QOS system are handled.
- Weighted Random Early Detection (WRED) can be configured globally to avoid congestion and drop the Yellow Frames (frames with Drop Probability (DP) set to 1) when the queues are filled.
- For controlling the amount of flooded frames entering the switch Storm Policers can be used at the global level.

QoS Classification

There are two methods of classification to a QoS Class (CoS): Basic and Advanced.

Basic QoS Classification

Basic QoS classification enables predefined schemes for handling Priority Code Points (PCP), Drop

Eligible Indicator (DEI), and Differentiated Service Code Points (DSCP):

- QoS classification based on PCP and DEI for tagged frames. The mapping table from PCP
- and DEI to QoS class is programmable per port.
- QoS classification based on DSCP values.
- DSCP Translation.
- DSCP Remarking based on QOS class.
- Per Port QOS class configuration for untagged and non IP Frames.

Advanced QoS Classification

Advanced QoS classification uses the QoS Control Lists (QCLs), which provide a flexible classification:

- Higher layer protocol fields (Layer 2 through Layer 4) for rule matching.
- Actions include mapping to QOS class and translation of PCP, DEI and DSCP values.

Policers

Policers limit the bandwidth of received frames exceeding the configurable rates. Policers can be configured at queue level or at a port level. There is also a provision to add policers at the EVC level, although this provision is not discussed in this document.

Shapers

Egress traffic shaping can be achieved using bandwidth shapers. Shapers can be configured at queue level or at a port level.

Scheduling Algorithm

Two types of scheduling are possible on the switch at a port level, Strict Priority and Deficit Weighted Round Robin (DWRR).

Strict Priority: All queues follow strict priority scheduling.

DWRR: Scheduling is based on the weights configured for each queue. Configuration is present to select the number of queues which can be under DWRR. It is possible to include from 2 to all 8 queues in DWRR mode.

When the number of queues selected for DWRR is less than 8 then the lowest priority queues are put in DWRR and higher priority queues are put in Strict Priority. For example, if number of Queues is 2 for DWRR then Queue 0 and 1 are set in DWRR mode and remaining Queues 2 to 8 are set in Strict Priority.

Weighted Random Early Detection (WRED) can be configured globally to avoid congestion and drop the Yellow Frames (frames with Drop Probability (DP) set to 1) when the queues are filled. For controlling the amount of flooded frames entering the switch Storm Policers can be used at global level.

Weighted Random Early Detection (WRED)

Congestion can be avoided in the queue system by enabling and configuring the Weighted Random Early Detection Function (WRED). WRED can discard the frames with Drop Probability set to 1. Configuration includes enabling WRED per queue (Global settings and not per port) and setting the Minimum and Maximum Threshold. Minimum threshold is the queue fill level at which the WRED. starts discarding the Frames. Maximum threshold can be configured either as Drop Probability or Fill Level. When the Unit is Drop Probability the mentioned threshold would be the Drop Probability with the queue fill level is just about 100%. When the Unit is Fill level, then it represents the Queue fill level where Drop probability is 100%.

Storm Policing

Storm Policers restrict the amount of flooded frames (Frames coming with SMAC which is not learnt earlier) entering the switch. The configurations are global per switch and not per port. Storm policer can be applied separately on Unicast, Multicast, or Broadcast packets.

QoS Configuration Examples

This section provides web GUI and ICLI configuration examples according to the different QoS classifications.

Note: To configure any of the following examples, first use the following command to restore system defaults.

```
# reload defaults
#
```

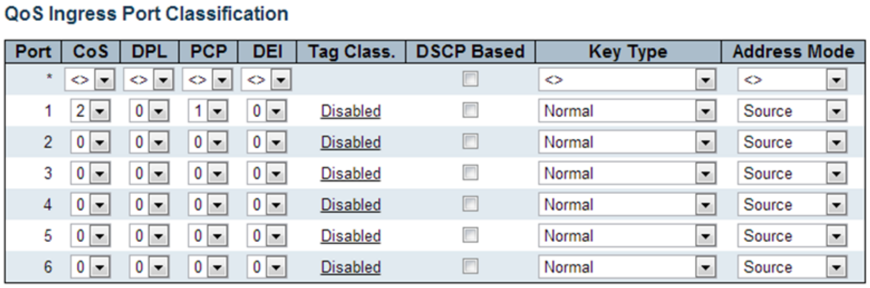
Port Classification

Basic QoS classification configuration can be done per port. Ingress traffic coming on each port can be assigned to a CoS, PCP, Drop Precedence Level (DPL), and DEI.

Example

All traffic coming on port 1 is mapped to CoS 2 and PCP is set as 1.

Click **Configuration** > **QoS** > **Port Classification** and enter the following settings.



QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Key Type	Address Mode
*	<>	<>	<>	<>		☐	<>	<>
1	2	0	1	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

***Figure 1* • QoS Ingress Port Classification**

The equivalent ICLI commands are as follows:

```
# configure terminal
(config)# interface GigabitEthernet 1/1
! Set Cos to 2 and PCP to 1
(config-if)# qos cos 2
(config-if)# qos pcp 1
(config-if)# end
```

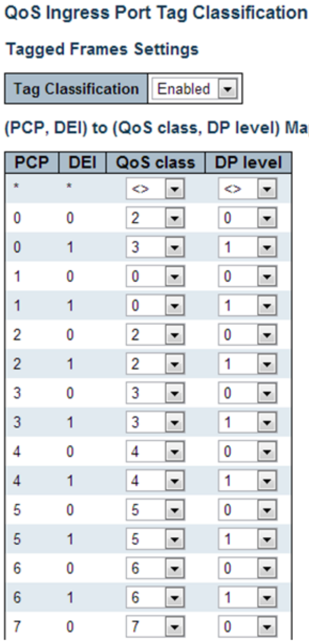
Tagged Frame Classification per Port

Ingress port tag classification can be done based on the PCP and DEI values received on the incoming packets. This is done by enabling tag classification for that port.

Example

Map PCP 0 and DEI 0 to QoS Class 2, Map PCP 0 and DEI 1 to QoS Class 3 on port 2.

Click **Configuration** > **QoS** > **Port Classification**, **Tag Class** and enter the following settings.



QoS Ingress Port Tag Classification Port 2

Tagged Frames Settings

Tag Classification	Enabled

(PCP, DEI) to (QoS class, DP level) Mapping

PCP	DEI	QoS class	DP level
*	*	<>	<>
0	0	2	0
0	1	3	1
1	0	0	0
1	1	0	1
2	0	2	0
2	1	2	1
3	0	3	0
3	1	3	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0

Figure 2 • **QoS Ingress Port Tag Classification**

The equivalent ICLI commands are as follows:

```
# configure terminal
(config)# interface GigabitEthernet 1/2
! Enable Tag Classification
(config-if)# qos trust tag
! Map PCP 0 and DEI 0 to Qos Class 2
(config-if)# qos map tag-cos pcp 0 dei 0 cos 2 dpl 0
! Map PCP 0 and DEL 1 to Qos Class 3
(config-if)# qos map tag-cos pcp 0 dei 1 cos 3 dpl 1
(config-if)# end
```

Tag Remarking per Port

Tag remarking on the egress frames can be done in the following three ways.

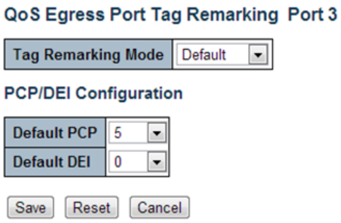
1. Classified: PCP and DEI values on the egress frames are updated with the classified values at the ingress. By default the PCP and DEI values are set to classified values.
2. Default: PCP and DEI values on the egress frames are updated to default values defined per port.
3. Mapped: PCP and DEI values on the egress frames are updated based on the tag remarking QoS/DPL to PCP/DEI Mapping per port.

PCP and DEI values sent on the egress frames can be mapped to QoS class and DPL values. This configuration can be done per port.

Example 1

Set Default PCP to 5 and DEI to 0 on port 3.

Click **Configuration** > **QoS** > **Port Tag Remarking**, **Port No** and enter the following settings.



QoS Egress Port Tag Remarking Port 3

Tag Remarking Mode	Default

PCP/DEI Configuration

Default PCP	5
Default DEI	0

Figure 3 **• QoS Egress Port Tag Remarking Port 3**

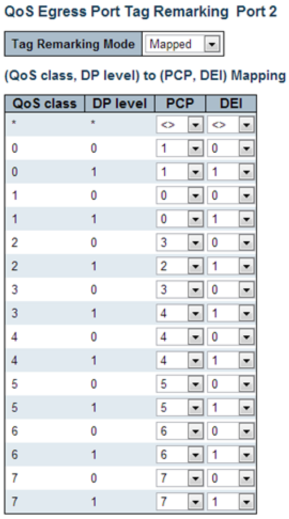
The equivalent ICLI commands are as follows:

```
# configure terminal
(config)# interface GigabitEthernet 1/3
! Set Default PCP to 5 and DEI to 0
(config-if)# qos tag-remark pcp 5 dei 0
(config-if)# end
```

Example 2

Map QoS Class 2 and DPL 0 to PCP 3 and DEI 0. Map QoS Class 3 and DPL 1 to PCP 4 and DEI 1.

Click **Configuration** > **QoS** > **Port Tag Remarking**, **Port No** and enter the following settings.



QoS Egress Port Tag Remarking Port 2

Tag Remarking Mode	Mapped

(QoS class, DP level) to (PCP, DEI) Mapping

QoS class	DP level	PCP	DEI
*	*	<>	<>
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	3	0
2	1	2	1
3	0	3	0
3	1	4	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0
7	1	7	1

Figure 4 **• QoS Egress Port Tag Remarking Port 2**

The equivalent ICLI commands are as follows:

```
# configure terminal
(config)# interface GigabitEthernet 1/2
! Set Tag Remarking to Mapped
(config-if)# qos tag-remark mapped
! Map QoS Class 2 and DPL 0 to PCP 3 and DEI 0
(config-if)# qos map cos-tag cos 2 dpl 0 pcp 3 dei 0
! Map QoS Class 3 and DPL 1 to PCP 4 and DEI 1
```

```
(config-if)# qos map cos-tag cos 3 dpl 1 pcp 4 dei 1
(config-if)# end
```

DSCP Configuration

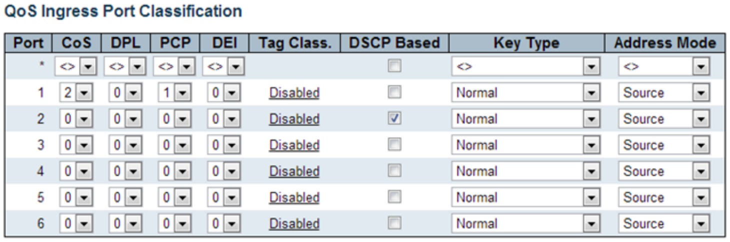
The following DSCP Configuration settings are present per port for ingress and egress.

1. DSCP based QoS classification
2. Selection of trusted DSCP values used for QoS classification
3. DSCP Translation: DSCP translation is done based on the DSCP translation table
4. Classify (For rewriting if enabled):
   - No DSCP classification
   - Classify only DSCP=0
   - Classify only selected (trusted) DSCP values based on the DSCP classification table
   - Classify all DSCP
5. Rewrite (on egress):
   - No egress rewrite
   - Rewrite enabled without remapping
   - Remap DSCP with DP unaware
   - Remap DSCP with DP aware

Example 1

DSCP (only trusted) to QoS class / DPL classification at ingress on port 2.

Check the DSCP Based box at **Configuration** > **QoS** > **Port Classification**.

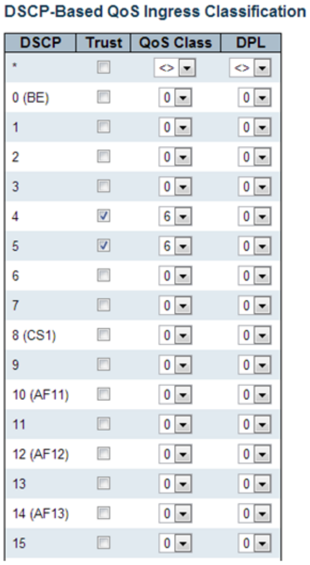


QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Key Type	Address Mode
*	<>	<>	<>	<>		□	<>	<>
1	2	0	1	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

Figure 5 • **QoS Ingress Port Classification**

Click **Configuration** > **QoS** > **DSCP-Based QoS**.



DSCP-Based QoS Ingress Classification

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

Figure 6 • **DSCP-Based QoS Ingress Classification**

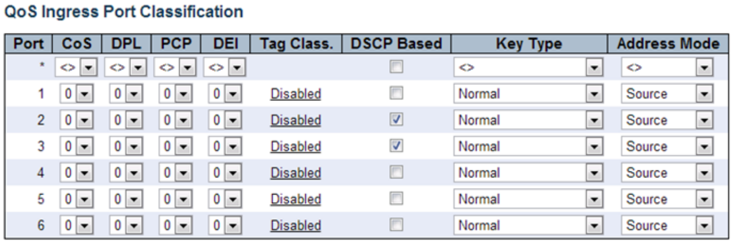
The equivalent ICLI commands are as follows:

```
# configure terminal
! Enable DSCP Trust for DSCP at Port 2.
(config)# interface GigabitEthernet 1/2
(config-if)# qos trust dscp
(config-if)# exit
! Map DSCP Values 4 and 5 to QoS Class 6.
(config)# qos map dscp-cos 4 cos 6 dpl 0
(config)# qos map dscp-cos 5 cos 6 dpl 0
(config)# end
```

Example 2

Translate DSCP at ingress on port 2 and rewrite enabled on port 3.

Check the DSCP Based box at **Configuration** > **QoS** > **Port Classification**.

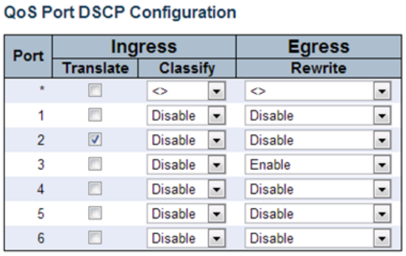


QoS Ingress Port Classification

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

Figure 7 • **QoS Ingress Port Classification**

Check the Translate box at **Configuration** > **QoS** > **Port DSCP**.

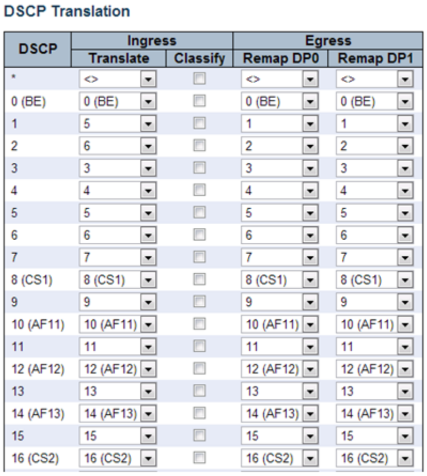


QoS Port DSCP Configuration

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

Figure 8 • **QoS Port DSCP Configuration**

Click **Configuration** > **QoS** > **DSCP** Translation and enter the following translation mapping.



DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	□	<>	<>
0 (BE)	0 (BE)	□	0 (BE)	0 (BE)
1	5	□	1	1
2	6	□	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)

Figure 9 • **DCP Translation**

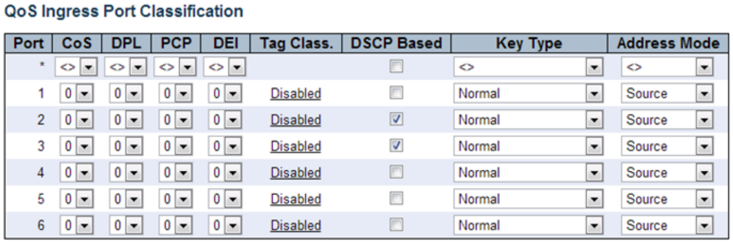
The equivalent ICLI commands are as follows:

```
# configure terminal
! Enable DSCP Translate at ingress on Port 2
(config)# interface GigabitEthernet 1/2
(config-if)# qos trust dscp
(config-if)# qos dscp-translate
(config-if)# exit
! Enable DSCP Remark at egress on Port 3
(config)# interface GigabitEthernet 1/3
(config-if)# qos trust dscp
(config-if)# qos dscp-remark rewrite
(config-if)# exit
! Create Ingress DSCP Translation Map
(config)# qos map dscp-ingress-translation 1 to 5
(config)# qos map dscp-ingress-translation 2 to 6
(config)# end
```

Example 3

Classify only DSCP = 0 at ingress on port 2 and rewrite enabled on port 3.

Check the DSCP Based box at **Configuration** > **QoS** > **Port Classification**.

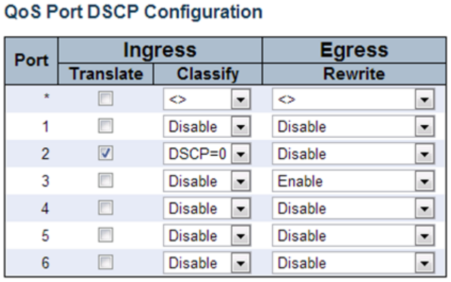


QoS Ingress Port Classification

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

Figure 10 **• QoS Ingress Port Classification**

Set the Ingress values at **Configuration** > **QoS** > **Port DSCP**.

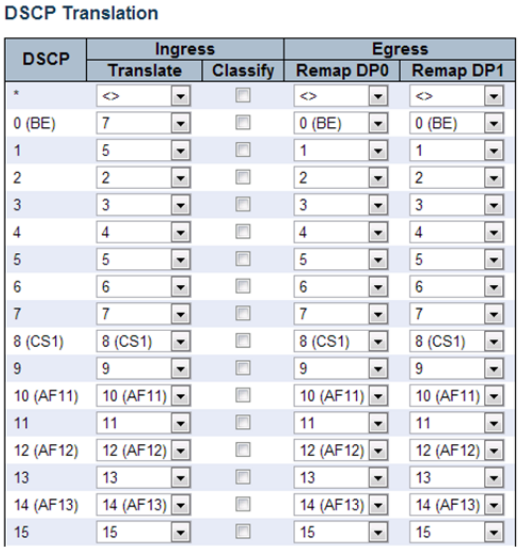


QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	□	<>	<>
1	□	Disable	Disable
2	☑	DSCP=0	Disable
3	□	Disable	Enable
4	□	Disable	Disable
5	□	Disable	Disable
6	□	Disable	Disable

Figure 11 **• QoS Port DSCP Configuration**

Click **Configuration** > **QoS** > **DSCP** Translation and enter the following translation mapping.



DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	□	<>	<>
0 (BE)	7	□	0 (BE)	0 (BE)
1	5	□	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

Figure 12 **• DSCP Translation**

The equivalent ICLI commands are as follows:

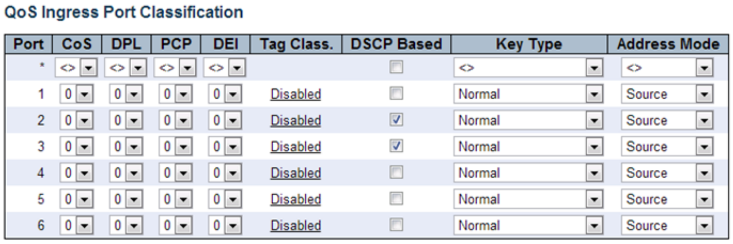
```
# configure terminal
! Enable DSCP=0 Classification and Translation at ingress on Port 2
(config)# interface GigabitEthernet 1/2
(config-if)# qos trust dscp
(config-if)# qos dscp-classify zero
```

```
(config-if)# qos dscp-translate
(config-if)# exit
! Create Ingress DSCP Translation Map.
(config)# qos map dscp-ingress-translation 0 to 7
(config)# qos map dscp-ingress-translation 1 to 5
! Note: Only DSCP=0 will be rewritten as these are only classified.
! Enable DSCP Remark at egress on Port 3
(config)# interface GigabitEthernet 1/3
(config-if)# qos trust dscp
(config-if)# qos dscp-remark rewrite
(config-if)# exit
(config)# end
```

Example 4

Classify Selected DSCP at ingress on port 2, DSCP rewrite enabled on port 3.

Check the DSCP Based box at **Configuration** > **QoS** > **Port Classification**.

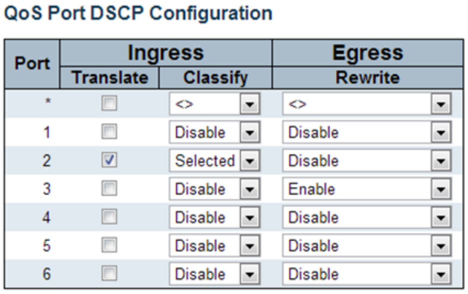


QoS Ingress Port Classification

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

Figure 13 • **QoS Ingress Port Classification**

Set the values at **Configuration** > **QoS** > **Port DSCP**.

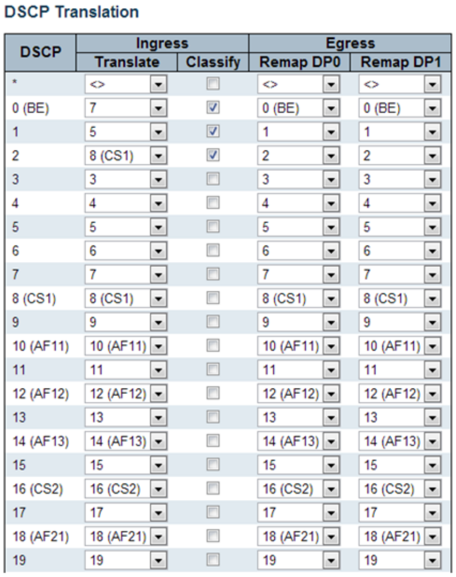


QoS Port DSCP Configuration

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

Figure 14 • **QoS Port DSCP Configuration**

Click **Configuration** > **QoS** > **DSCP** Translation and enter the following translation mapping.



DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	□	<>	<>
0 (BE)	7	☑	0 (BE)	0 (BE)
1	5	☑	1	1
2	8 (CS1)	☑	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

Figure 15 **• DSCP Translation**

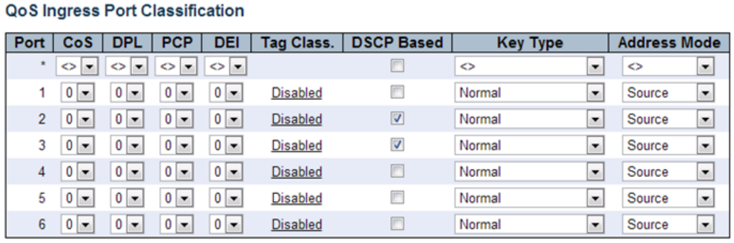
The equivalent ICLI commands are as follows:

```
# configure terminal
! Enable DSCP classification for selected DSCP values at ingress Port 2
(config)# interface GigabitEthernet 1/2
(config-if)# qos trust dscp
(config-if)# qos dscp-classify selected
(config-if)# exit
(config)# qos map dscp-classify 0
(config)# qos map dscp-classify 1
(config)# qos map dscp-classify 2
! Create Ingress DSCP Translation Map.
(config)# qos map dscp-ingress-translation 0 to 7
(config)# qos map dscp-ingress-translation 1 to 5
(config)# qos map dscp-ingress-translation 2 to 8
! Enable DSCP Remark at egress on Port 3
(config)# interface GigabitEthernet 1/3
(config-if)# qos trust dscp
(config-if)# qos dscp-remark rewrite
(config-if)# exit
(config-if)# end
```

Example 5

Classify all DSCP values at ingress on port 2, rewrite enabled on port 3.

Check the DSCP Based box at **Configuration** > **QoS** > **Port Classification**.

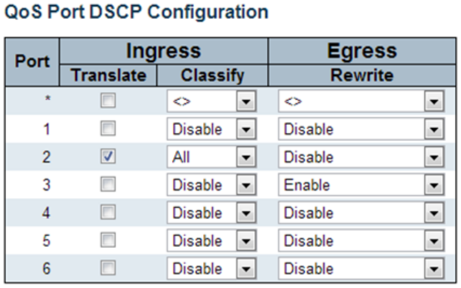


QoS Ingress Port Classification

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

***Figure 16* • QoS Ingress Port Classification**

Set the values at **Configuration** > **QoS** > **Port DSCP**.



QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	☐	<>	<>
1	☐	Disable	Disable
2	☑	All	Disable
3	☐	Disable	Enable
4	☐	Disable	Disable
5	☐	Disable	Disable
6	☐	Disable	Disable

***Figure 17* • QoS Port DSCP Configuration**

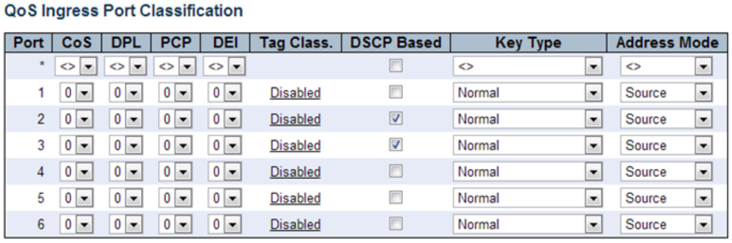
The equivalent ICLI commands are as follows:

```
# configure terminal
! Enable DSCP classification for all DSCP values at ingress Port 2
(config)# interface GigabitEthernet 1/2
(config-if)# qos trust dscp
(config-if)# qos dscp-classify any
(config-if)# exit
! Enable DSCP Remark at egress on Port 3
(config)# interface GigabitEthernet 1/3
(config-if)# qos trust dscp
(config-if)# qos dscp-remark rewrite
(config-if)# exit
(config)# end
```

Example 6

QoS/DP to DSCP Classification enabled. Rewrite DSCP with DP Aware at egress on port 3.

Check the DSCP Based box at **Configuration** > **QoS** > **Port Classification**.

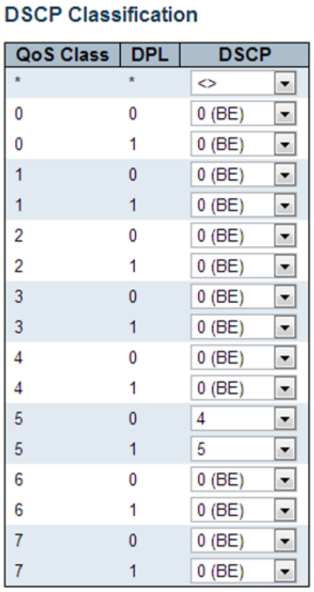


QoS Ingress Port Classification

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

Figure 18 **• QoS Ingress Port Classification**

Click **Configuration** > **QoS** > **DSCP Classification** and enter the following settings.

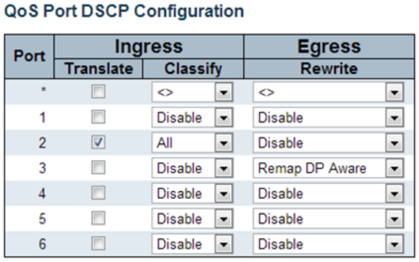


DSCP Classification

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	4
5	1	5
6	0	0 (BE)
6	1	0 (BE)
7	0	0 (BE)
7	1	0 (BE)

Figure 19 **• DSCP Classification**

Set the values at **Configuration** > **QoS** > **Port DSCP**.

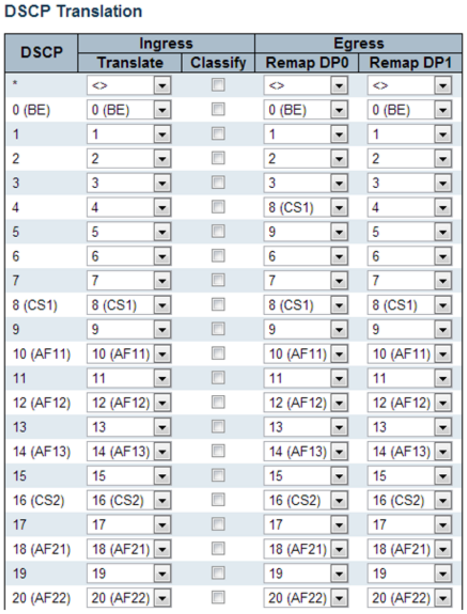


QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	□	<>	<>
1	□	Disable	Disable
2	☑	All	Disable
3	□	Disable	Remap DP Aware
4	□	Disable	Disable
5	□	Disable	Disable
6	□	Disable	Disable

Figure 20 **• QoS Port DSCP Configuration**

Click **Configuration** > **QoS** > **DSCP** Translation and enter the following translation mapping.



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	□	8 (CS1)	4
5	5	□	9	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)

Figure 21 **• DSCP Translation**

Note To execute this example PCP/DEI on the incoming packets can be used to direct packets to a particular QoS class and DP value, .

The equivalent ICLI commands are as follows:

```
# configure terminal
! Enable DSCP Classification on all DSCP values on port 2.
(config)# interface GigabitEthernet 1/2
(config-if)# qos trust dscp
(config-if)# qos dscp-classify any
(config-if)# exit
! Map QoS Class 5, DP = 0 to DSCP 4, QoS Class 5, DP = 1 to DSCP 5
(config)# qos map cos-dscp 5 dpl 0 dscp 4
(config)# qos map cos-dscp 5 dpl 1 dscp 5
! Remap DSCP 4, DP = 0 to DSCP = 8 and DSCP 5, DP = 1 to DSCP =9 on Egress
(config)# qos map dscp-egress-translation 4 0 to 8
(config)# qos map dscp-egress-translation 5 0 to 9
! Enable DSCP rewrite with DSCP Remap DP Aware on Port 3
(config)# interface GigabitEthernet 1/3
(config-if)# qos dscp-remark remap-dp
(config-if)# end
```

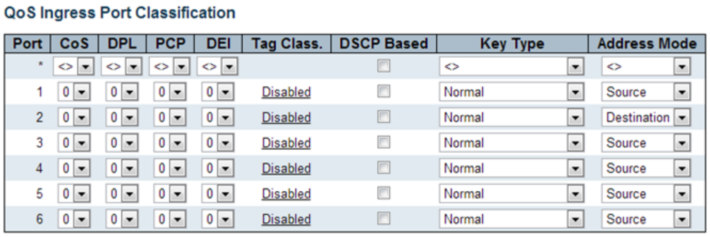
QCLs

Advanced QoS classification can be done by checking fields from Layer 2 to Layer 4 and mapping them to PCP/DEI, QoS class and DSCP values.

Example 1

Match on a particular destination MAC on port 2 and map these to QoS class 5

Set the Address Mode at **Configuration** > **QoS** > **Port Classification**.

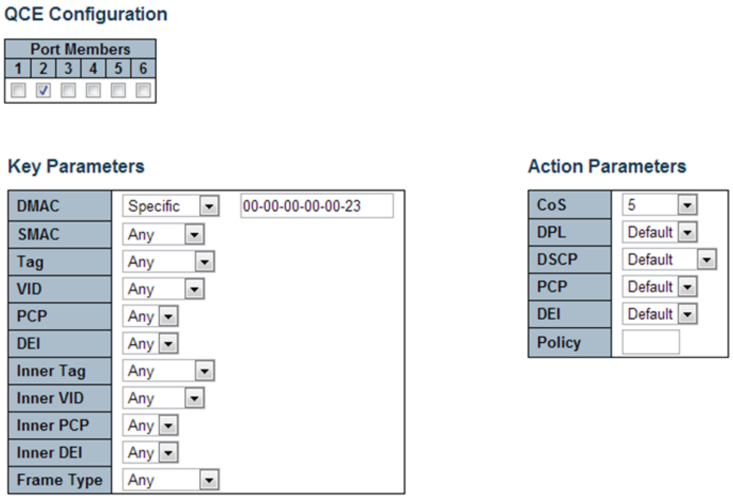


QoS Ingress Port Classification

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	Destination
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

Figure 22 • **QoS Ingress Port Classification**

Set the Port and Class at **Configuration** > **QoS** > **QoS Control List**.



QCE Configuration

Port Members					
1	2	3	4	5	6
□	☑	□	□	□	□

Key Parameters

DMAC	Specific	00-00-00-00-00-23
SMAC	Any	
Tag	Any	
VID	Any	
PCP	Any	
DEI	Any	
Inner Tag	Any	
Inner VID	Any	
Inner PCP	Any	
Inner DEI	Any	
Frame Type	Any	

Action Parameters

CoS	5
DPL	Default
DSCP	Default
PCP	Default
DEI	Default
Policy	

Figure 23 • **QoS Control List**

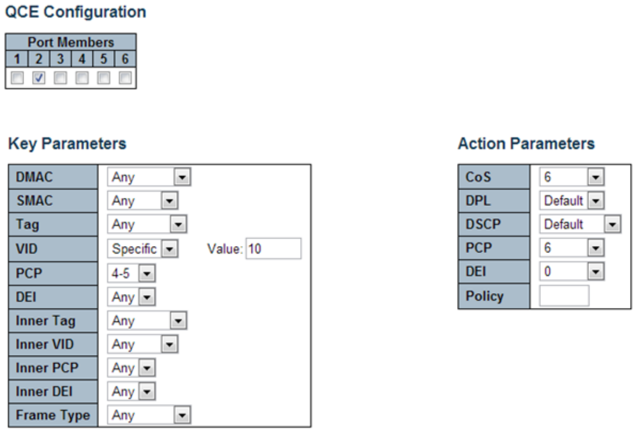
The equivalent ICLI commands are as follows:

```
# configure terminal
! Set the Address mode to Destination on Port 2
(config)# interface GigabitEthernet 1/2
(config-if)# qos qce addr destination
(config-if)# exit
! Create QCL rule for matching particular destination MAC on Port 2
(config)# qos qce 1 interface GigabitEthernet 1/2 dmac 00-00-00-00-00-23 action
cos 5
(config-if)# end
```

Example 2

Match on a particular VLAN Tag and PCP range on port 2 and map these to QoS class 6. Also map these frames to PCP = 6 and DEI = 0.

Set the appropriate values at **Configuration** > **QoS** > **QoS Control List**.



QCE Configuration

Port Members					
1	2	3	4	5	6
□	☑	□	□	□	□

Key Parameters

DMAC	Any	
SMAC	Any	
Tag	Any	
VID	Specific	Value: 10
PCP	4-5	
DEI	Any	
Inner Tag	Any	
Inner VID	Any	
Inner PCP	Any	
Inner DEI	Any	
Frame Type	Any	

Action Parameters

CoS	6
DPL	Default
DSCP	Default
PCP	6
DEI	0
Policy	

Figure 24 • **QoS Control List**

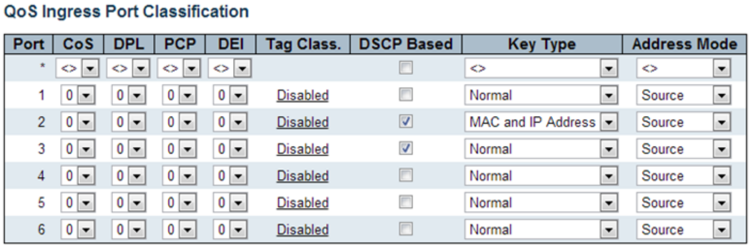
The equivalent ICLI commands are as follows:

```
# configure terminal
! Create QCL rule for matching particular VLAN ID and range of PCP values.
(config)# qos qce 1 interface GigabitEthernet 1/2 tag vid 10 pcp 4-5 action
cos 6 pcp-dei 6 (config)# end
```

Example 3

Match on specific Dest MAC, Source IP, UDP SPort number on port 2. Map these to QoS Class 7, DP = 1 and DSCP value = 9.

Set the values at **Configuration** > **QoS** > **Port Classification** as follows:

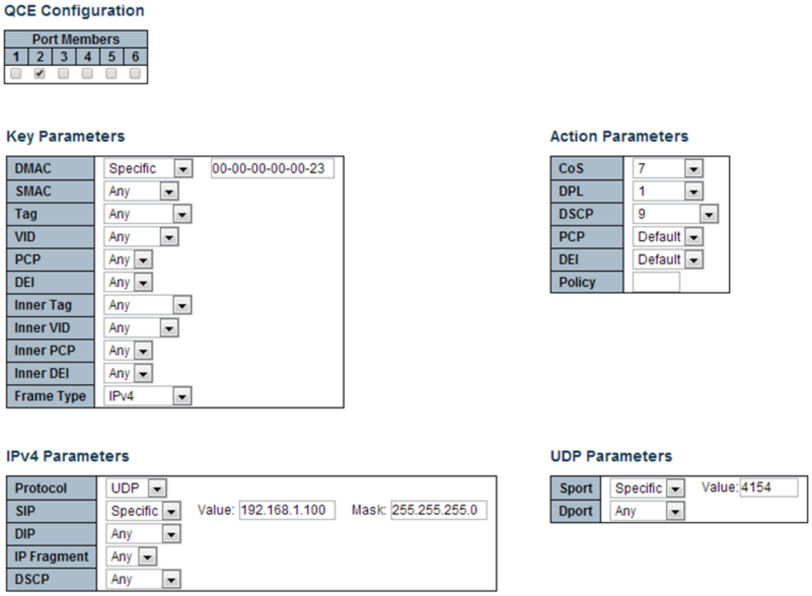


QoS Ingress Port Classification

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	☑	MAC and IP Address	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

Figure 25 • **QoS Ingress Port Classification**

Create the appropriate QCL at **Configuration** > **QoS** > **QoS Control List**.



QCE Configuration

Port Members					
1	2	3	4	5	6
□	☑	□	□	□	□

Key Parameters

DMAC	Specific	00-00-00-00-00-23
SMAC	Any	
Tag	Any	
VID	Any	
PCP	Any	
DEI	Any	
Inner Tag	Any	
Inner VID	Any	
Inner PCP	Any	
Inner DEI	Any	
Frame Type	IPv4	

Action Parameters

CoS	7
DPL	1
DSCP	9
PCP	Default
DEI	Default
Policy	

IPv4 Parameters

Protocol	UDP		
SIP	Specific	Value: 192.168.1.100	Mask: 255.255.255.0
DIP	Any		
IP Fragment	Any		
DSCP	Any		

UDP Parameters

Sport	Specific	Value: 4154
Dport	Any	

Figure 26 • **QoS Control List**

The equivalent ICLI commands are as follows:

```
# configure terminal
! Set the QCE address mode to MAC and IP address on Port 2.
(config)# interface GigabitEthernet 1/2
(config-if)# qos qce key mac_ip_addr
(config-if)# exit
! Create QCL rule for matching DMAC, SIP, UDP Sport on Port 2.
(config)# qos qce 1 interface GigabitEthernet 1/2 dmac 00-00-00-00-00-23
frame-type ipv4 proto (config)# end
```

Policers

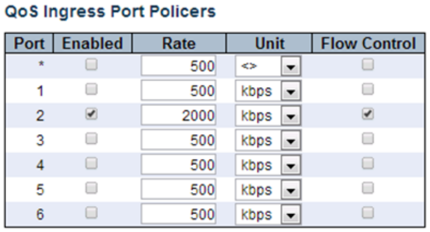
Port Policers

Enable policing at port level on a particular port.

Example 1

Enable policer on port 2 and set the policer rate to 2000 Kbps. For better performance, optionally enable flow control as well if the policed traffic is TCP traffic.

Set the policer rate at **Configuration** > **QoS** > **Port Policing**.



QoS Ingress Port Policers

Port	Enabled	Rate	Unit	Flow Control
*	□	500	<>	□
1	□	500	kbps	□
2	☑	2000	kbps	☑
3	□	500	kbps	□
4	□	500	kbps	□
5	□	500	kbps	□
6	□	500	kbps	□

Figure 27 • **QoS Ingress Port Policers**

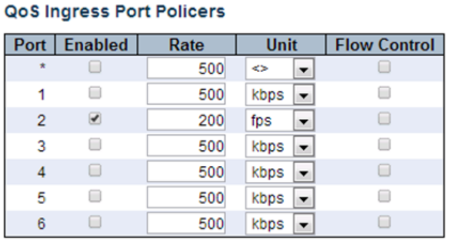
The equivalent ICLI commands are as follows:

```
# configure terminal
! Enable Policer on Port 2 with a rate set to 2000Kbps
(config)# interface GigabitEthernet 1/2
(config-if)# qos policer 2000 flowcontrol
(config-if)# end
```

Example 2

Enable policer on port 2 and set the policer rate to 200 fps. The units are frames per second.

Set the policer rate at **Configuration** > **QoS** > **Port Policing**.



QoS Ingress Port Policers

Port	Enabled	Rate	Unit	Flow Control
*	□	500	<>	□
1	□	500	kbps	□
2	☑	200	fps	□
3	□	500	kbps	□
4	□	500	kbps	□
5	□	500	kbps	□
6	□	500	kbps	□

Figure 28 • **QoS Ingress Port Policers**

The equivalent ICLI commands are as follows:

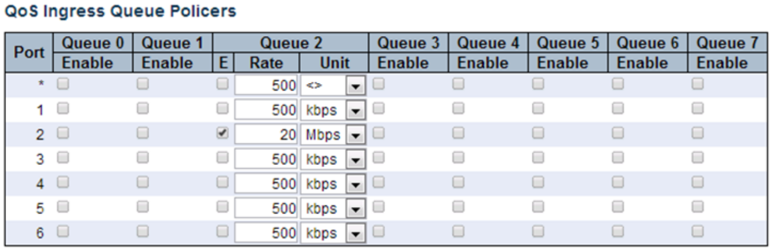
```
# configure terminal
! Enable Policer on Port 2 with a rate set to 200fps
(config)# interface GigabitEthernet 1/2
(config-if)# qos policer 200 fps
(config-if)# end
```

Queue Policers

Example

Enable policer on queue 2 at port 2. Set the policing rate to 20 Mbps.

Configure the policer at **Configuration** > **QoS** > **Queue Policing** as follows:



QoS Ingress Queue Policers

Port	Queue 0	Queue 1	Queue 2			Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	Enable	Enable	E	Rate	Unit	Enable	Enable	Enable	Enable	Enable
*	☐	☐	☐	500	<>	☐	☐	☐	☐	☐
1	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
2	☐	☐	☑	20	Mbps	☐	☐	☐	☐	☐
3	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
4	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
5	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
6	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐

Figure 29 • **QoS Ingress Queue Policers**

The equivalent ICLI commands are as follows:

```
# configure terminal
! Enable Policer on Queue 2 at Port 2 with a rate set to 20 Mbps
(config)# interface GigabitEthernet 1/2
(config-if)# qos queue-policer queue 2 20000
(config-if)# end
```

Shapers

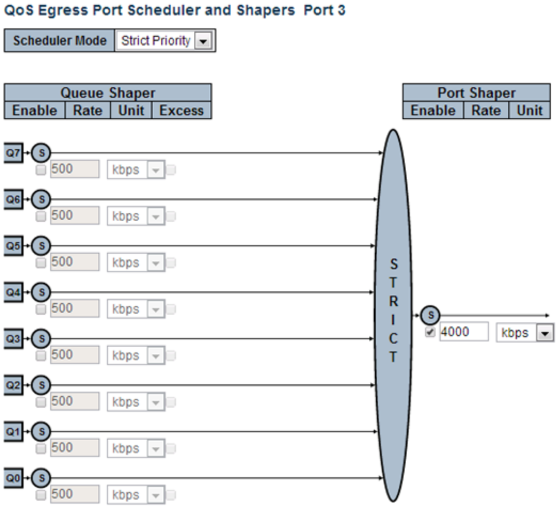
Port Shapers

Enable shapers at port level to shape the egress traffic.

Example

Enable shaper on port 3 and set the shaping rate to 4000 Kbps.

Set the Scheduler Mode and rate at **Configuration** > **QoS** > **Port Shaping**, **Port No**.



QoS Egress Port Scheduler and Shapers Port 3

Scheduler Mode: Strict Priority

Queue	Queue Shaper Enable	Rate	Unit	Excess
Q7	☐	500	kbps	☐
Q6	☐	500	kbps	☐
Q5	☐	500	kbps	☐
Q4	☐	500	kbps	☐
Q3	☐	500	kbps	☐
Q2	☐	500	kbps	☐
Q1	☐	500	kbps	☐
Q0	☐	500	kbps	☐

Port Shaper Enable	Rate	Unit
☑	4000	kbps

Figure 30 • **QoS Egress Port Scheduler and Shapers Port 3**

The equivalent ICLI commands are as follows:

```
# configure terminal
! Enable Shaper on Port 3 and set the rate to 4000 Kbps
```

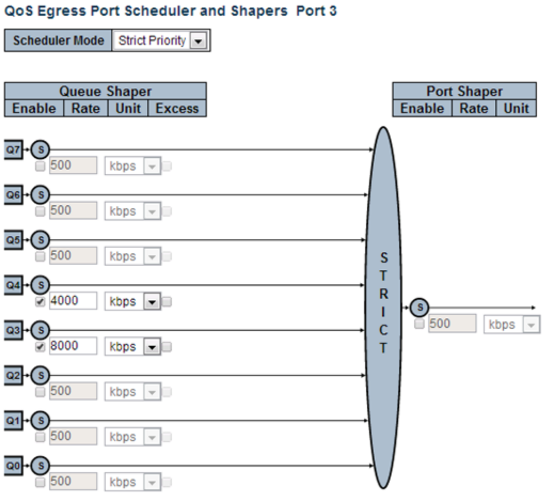
```
(config)# interface GigabitEthernet 1/3
(config-if)# qos shaper 4000
(config-if)# end
```

Queue Shapers

Example

Enable shaping on Queue 3 and Queue 4 at different rates on Port 3.

Set the shaper at **Configuration** > **QoS** > **Port Shaping**, **Port No** as follows:



QoS Egress Port Scheduler and Shapers Port 3

Scheduler Mode: Strict Priority

Queue	Queue Shaper Enable	Rate	Unit	Excess
Q7	□	500	kbps	□
Q6	□	500	kbps	□
Q5	□	500	kbps	□
Q4	☑	4000	kbps	□
Q3	☑	8000	kbps	□
Q2	□	500	kbps	□
Q1	□	500	kbps	□
Q0	□	500	kbps	□

Port Shaper Enable	Rate	Unit
□	500	kbps

Figure 31 • **QoS Egress Port Scheduler and Shapers Port 3**

The equivalent ICLI commands are as follows:

```
# configure terminal
! Enable Queue Shaper on Queues 3 and 4 on Port 3 and set the rate to 4000 and
8000 Kbps
(config)# interface GigabitEthernet 1/3
(config-if)# qos queue-shaper queue 3 4000
(config-if)# qos queue-shaper queue 4 8000
(config-if)# end
```

Schedulers

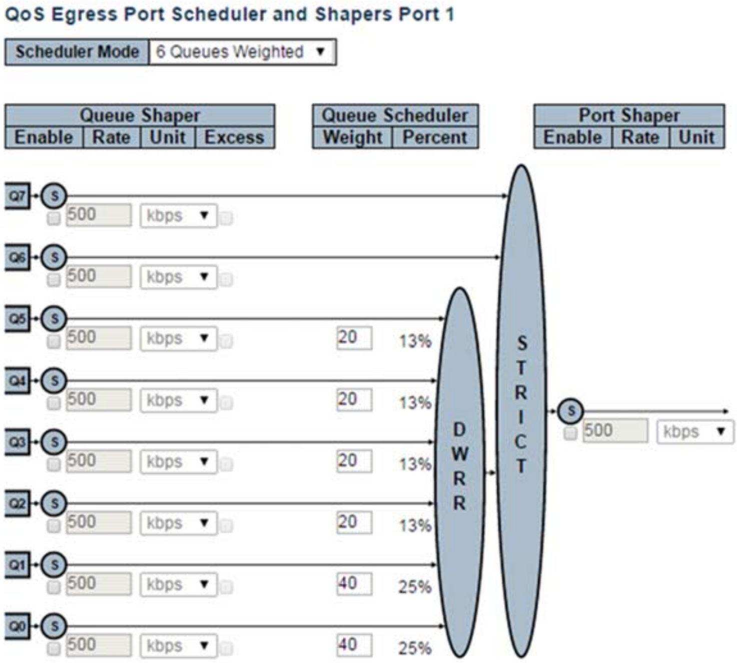
DWRR

Example

Set the scheduling mode to DWRR (for 6 queues) on Port 3 with the following weights:

Queue0- 40, Queue1-40, Queue2-20, Queue3-20, Queue4-20 and Queue5-20.

Configure the Scheduler at **Configuration** > **QoS** > **Port Shaping**, **Port No**.



QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: 6 Queues Weighted ▾

	Queue Shaper				Queue Scheduler	
	Enable	Rate	Unit	Excess	Weight	Percent
Q7	□	500	kbps ▾	□		
Q6	□	500	kbps ▾	□		
Q5	□	500	kbps ▾	□	20	13%
Q4	□	500	kbps ▾	□	20	13%
Q3	□	500	kbps ▾	□	20	13%
Q2	□	500	kbps ▾	□	20	13%
Q1	□	500	kbps ▾	□	40	25%
Q0	□	500	kbps ▾	□	40	25%

Port Shaper		
Enable	Rate	Unit
□	500	kbps ▾

Figure 32 • **QoS Egress Port Scheduler and Shapers Port 1**

The equivalent ICLI commands are as follows:

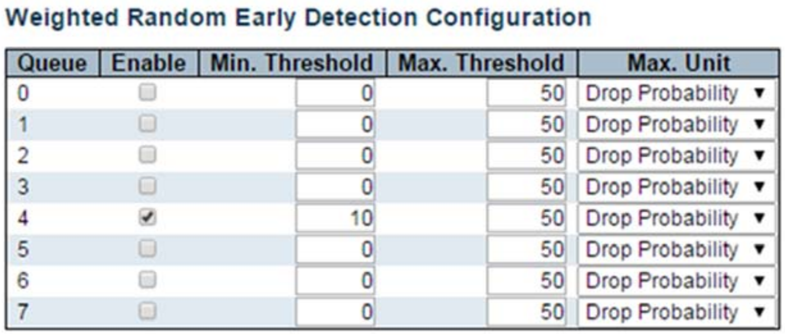
```
# configure terminal
! Set Scheduler mode to DWRR Priority on Port 3
(config)# interface GigabitEthernet 1/3
(config-if)# qos wrr 40 40 20 20 20 20
(config-if)# end
```

Weighted Random Early Detection (WRED)

Example 1

Configuring WRED on Queue 4 with a Minimum Threshold as 10% and Maximum Threshold as 50%. Maximum Threshold unit is Drop Probability.

Configure WRED at **Configuration** > **QoS** > **WRED**



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	☑	10	50	Drop Probability ▼
5	☐	0	50	Drop Probability ▼
6	☐	0	50	Drop Probability ▼
7	☐	0	50	Drop Probability ▼

***Figure 33* • Weighted Random Early Detection**

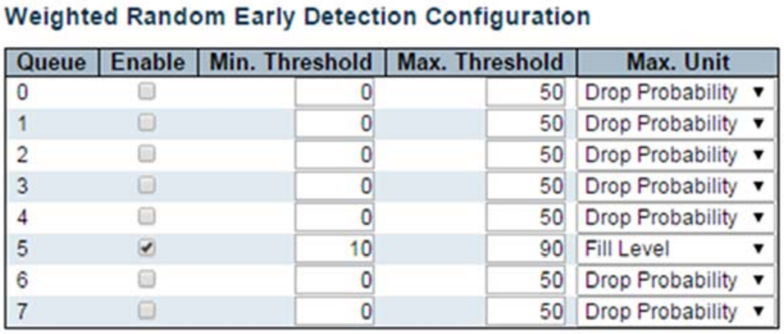
The equivalent ICLI Commands are:

```
# configure terminal
!Set Minimum threshold as 10 and Maximum Threshold as 50 on Queue 4.
(config)# qos wred queue 4 min-fl 10 max 50
```

Example 2

Configuring WRED on Queue 5 with a Minimum Threshold as 10% and Maximum Threshold as 90%. Maximum Threshold unit is Fill Level.

Configure WRED at **Configuration** > **QoS** > **WRED**



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	☑	10	90	Fill Level ▼
6	☐	0	50	Drop Probability ▼
7	☐	0	50	Drop Probability ▼

***Figure 34* • Weighted Random Early Detection**

The equivalent ICLI Commands are:

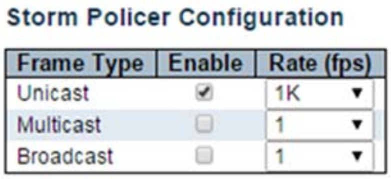
```
# configure terminal
!Set Minimum threshold as 10 and Maximum Threshold as 90 on Queue 5.
(config)# qos wred queue 5 min-fl 10 max 90 fill-level
```

Storm Policing

Example

Apply a storm policer of 1K fps on Unicast frame type.

Configure Storm Policer at **Configuration** > **QOS** > **Storm Policing**



Storm Policer Configuration

Frame Type	Enable	Rate (fps)
Unicast	☑	1K ▼
Multicast	□	1 ▼
Broadcast	□	1 ▼

Figure 35 • **Storm Policer Configuration**

The equivalent CLI Command is:

```
# configure terminal
(config)# qos storm unicast 1 kfps
```

CHAPTER 13

HQoS Configuration

This document provides examples on how to set up a Hierarchical Quality of Service (HQoS) using Industrial Command Line Interface (ICLI) commands on Cisco ME1200. The different scheduling modes have been outlined to describe the possible configurations.

This document is based on the ICLI configuration guide that describes the basic usage of the ME1200 ICLI and the QoS configuration guide that describes the basic usage of the QoS system.

Configuring the Port Scheduler using HQoS

With HQoS, the port scheduler can be configured in the following three different modes.

- Normal
- Basic
- Hierarchical

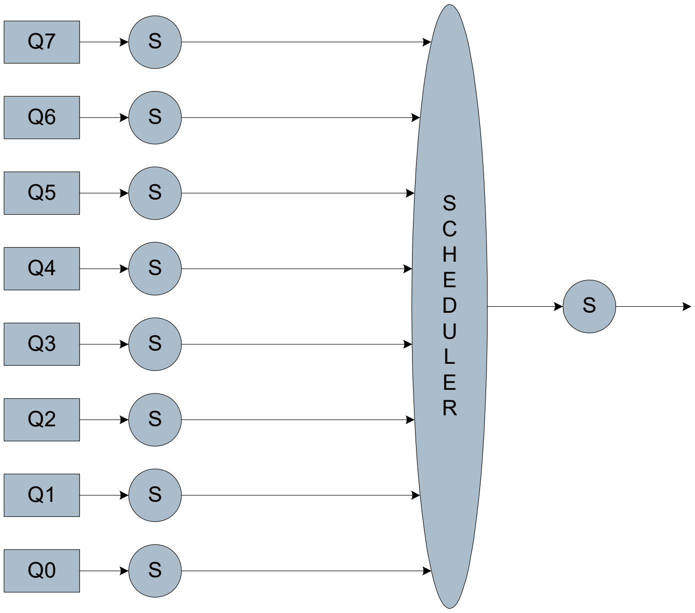
The modes define the available QoS features and also influence resource usage. A frame is always enqueued only in a single scheduling queue, independent of the scheduling mode.

Normal Scheduling Mode

Normal is the default scheduling mode for all ports and is the only available mode for Serval configurations without HQoS support.

The following illustration shows the normal scheduling mode where Qn represents queue (QoS class) n and S represents a shaper.

Figure 1 • **Normal Scheduling Mode**



The shapers after the queues are the queue shapers, and the rightmost shaper is the port shaper.

In normal mode, HQoS is disabled and all configurations of shapers and scheduler are handled by the regular QoS system.

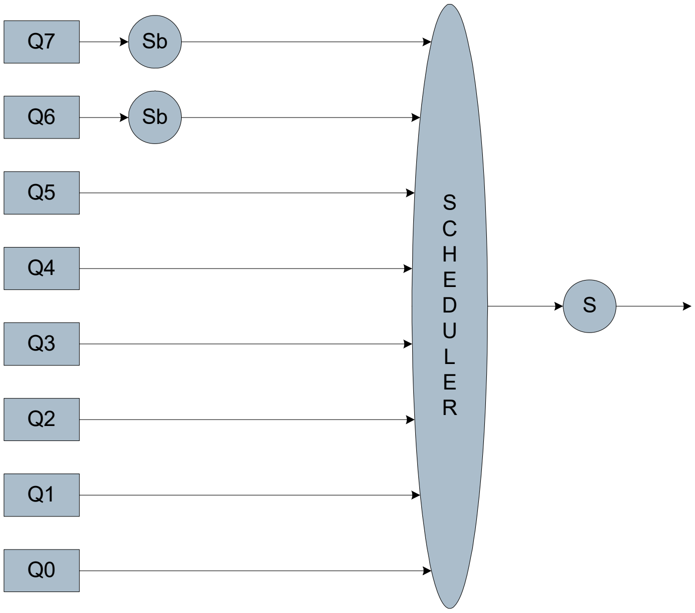
Basic Scheduling Mode

Basic mode supports fewer features than the normal mode but uses fewer resources. It is identical to normal mode with the following exceptions.

- Only queues 6 and 7 have queue shapers (the circles with Sb).
- The queue shapers do not support excess bandwidth.

The following illustration shows the basic scheduling mode.

Figure 2 • **Basic Scheduling Mode**



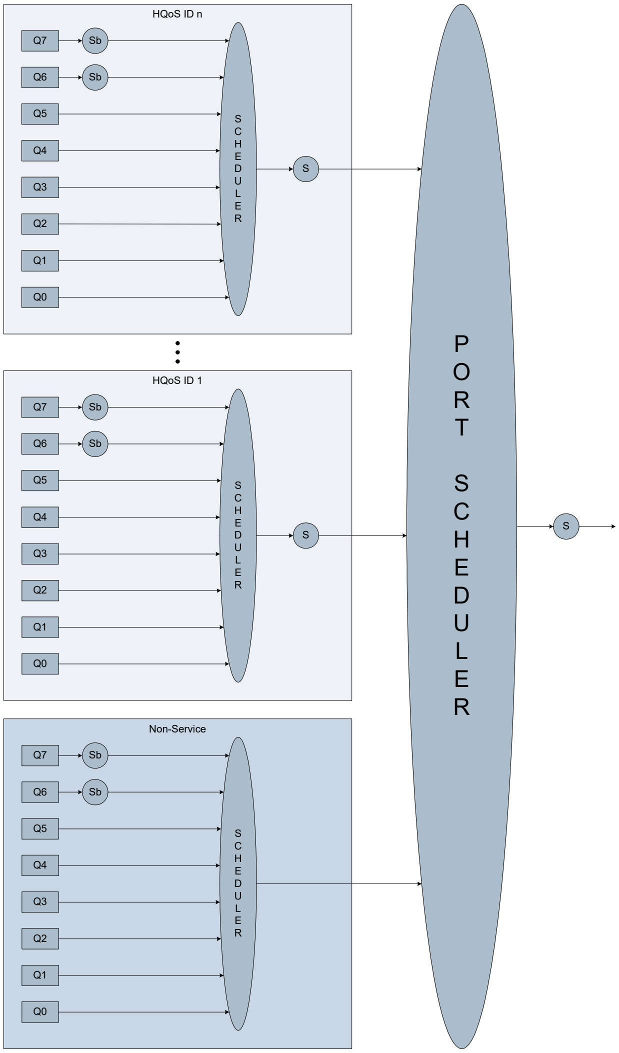
In basic mode, HQoS is disabled, and all configurations of shapers and scheduler are handled by the regular QoS system.

Hierarchical Scheduling Mode

Hierarchical mode allows for HQoS configuration. HQoS ID 1 to HQoS ID n are the HQoS profiles that are mapped to the port. Non-Service is the traffic that is not mapped to an HQoS profile. Each service that is using an HQoS profile is essentially a basic mode port (with an HQoS shaper instead of a port shaper) with the same shaper and scheduler configuration options.

The following illustration shows the hierarchical scheduling mode.

Figure 3 • **Hierarchical Scheduling Mode**



The regular QoS system configures the port shaper, queue shapers, and schedules for non-service traffic.

By default, the port scheduler is configured for fair round-robin scheduling between each HQoS profile and non-service traffic, but it can be weighted by configuring guaranteed bandwidths for the HQoS profile. When guaranteed bandwidth is configured for an HQoS profile, the remaining bandwidth of the port is equally divided between the remaining HQoS profiles and non-service traffic.

It is not possible to configure a guaranteed bandwidth for non-service traffic.

HQoS Configuration Examples

For more information about the models for the following ICLI configuration examples, see Understanding HQoS.

To configure any of the following examples, first use the following command to restore system defaults.

```
# reload defaults
```

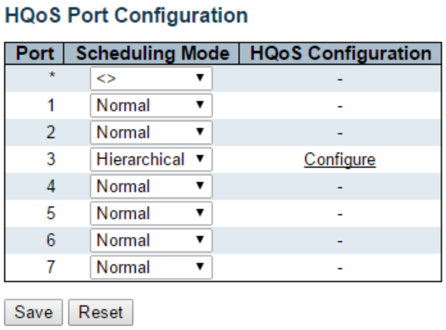
```
#
```

HQoS is enabled on a port when the interface is configured in hierarchical scheduling mode.

```
# configure terminal
! Configure Port 3 in Hierarchical Scheduling Mode
(config)# interface GigabitEthernet 1/3
(config-if)# hqos mode hierarchical
(config-if)# end
#
```

Web GUI configuration path: **Configuration > HQoS > Ports**.

Figure 4 • **HQoS Port Configuration**



HQoS Port Configuration

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

This can also be done after all the HQoS IDs and HQoS parameters are configured.

The following code snippet displays all possible HQoS commands with all possible parameters.

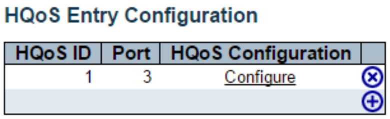
```
# configure terminal
! Show all HQoS related commands
(config)# hqos ??
hqos <hqos_id> guaranteed-bandwidth <rate>
hqos <hqos_id> interface <port_type> <port>
hqos <hqos_id> queue-shaper queue <queue> <rate> [ kbps | mbps ] [
rate-type { line | data } ]
hqos <hqos_id> shaper <rate> [ kbps | mbps ] [ rate-type { line | data } ]
hqos <hqos_id> wrr <w0> <w1> [ <w2> [ <w3> [ <w4> [ <w5> [ <w6> [ <w7>
] ] ] ] ] ]
(config)# end
#
```

An HQoS ID is created using the following interface command.

```
# configure terminal
! Create HQoS ID 1 on port 3
(config)# hqos 1 interface GigabitEthernet 1/3
(config)# end
#
```

Web GUI configuration path: **Configuration > HQoS > HQoS Entries, Add New HQoS Entry**.

Figure 5 • **HQoS Entry Configuration**



HQoS Entry Configuration

HQoS ID	Port	HQoS Configuration	
1	3	Configure	⊗
			⊕

Port Shaper

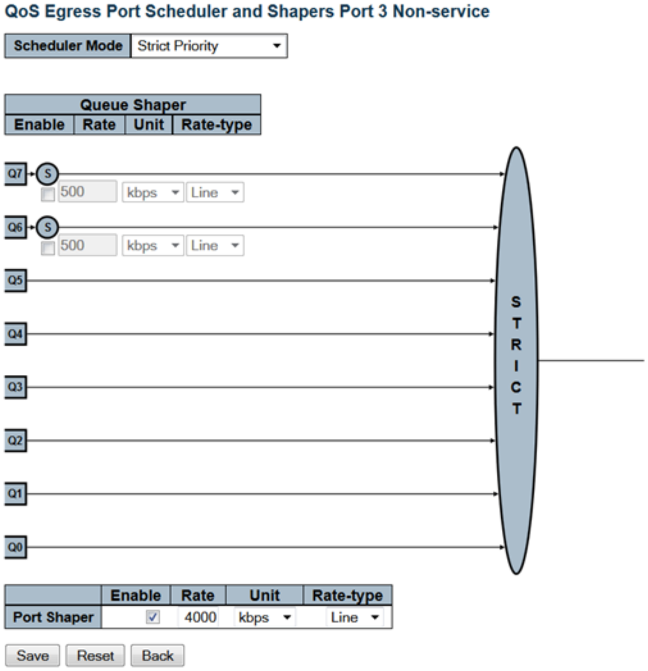
The port shaper is configured using the same commands whether or not HQoS is enabled.

The following example lists the commands to enable the port level shaper on port 3 and set the shaping rate to 4000 kbps (line rate).

```
# configure terminal
! Enable shaper on port 3 and set the rate to 4000 kbps
(config)# interface GigabitEthernet 1/3
(config-if)# qos shaper 4000
(config-if)# end
#
```

Web GUI configuration path: **Configuration > QoS > Port Shaping, Port No**.

Figure 6 • **Port Shaper**



QoS Egress Port Scheduler and Shapers Port 3 Non-service

Scheduler Mode	Strict Priority

Queue Shaper			
Enable	Rate	Unit	Rate-type

	Enable	Rate	Unit	Rate-type
Port Shaper	☑	4000	kbps	Line

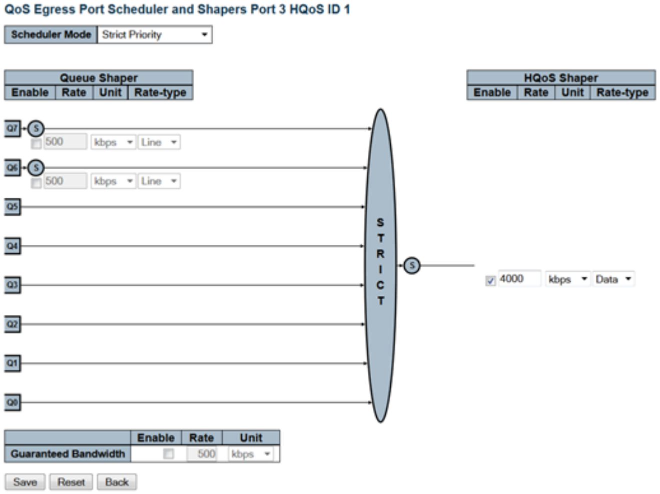
HQoS Shaper

The following example lists the commands to enable the HQoS level shaper for HQoS ID 1 on port 3 and set the shaping rate to 4000 kbps.

```
# configure terminal
! Enable HQoS shaper for HQoS ID 1 on port 3 and set the rate to 4000 kbps
(config)# hqos 1 shaper 4000 rate-type data
(config)# end
#
```

Web GUI configuration path: **Configuration > HQoS > HQoS Entries, Configure**

Figure 7 • **HQoS Shaper**



QoS Egress Port Scheduler and Shapers Port 3 HQoS ID 1

Scheduler Mode	Strict Priority

	Queue Shaper			
	Enable	Rate	Unit	Rate-type
Q7	□	500	kbps	Line
Q6	□	500	kbps	Line

HQoS Shaper			
Enable	Rate	Unit	Rate-type
☑	4000	kbps	Data

	Enable	Rate	Unit
Guaranteed Bandwidth	□	500	kbps

Non-service Queue Shaper

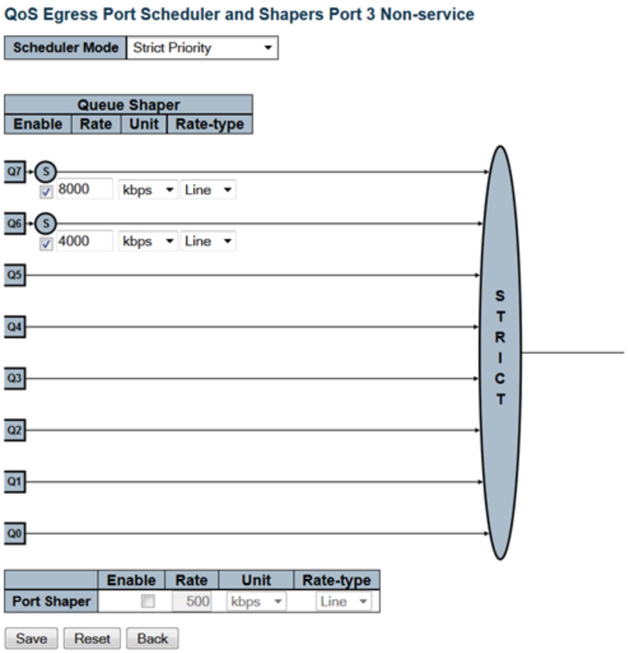
The non-service queue shapers are configured using the commands that configure the queue shapers when HQoS is disabled. When HQoS is enabled, only queue 6 and queue 7 have queue shapers.

The following example lists the commands to enable the non-service queue level shaper on queue 6 and queue 7 on port 3 and set the shaping rates to 4000 kbps and 8000 kbps respectively.

```
# configure terminal
! Enable non-service queue shapers on queues 6 and 7 on port 3 and set
the rate to 4000 kbps for queue 6 and 8000 kbps for queue 7
(config)# interface GigabitEthernet 1/3
(config-if)# qos queue-shaper queue 6 4000
(config-if)# qos queue-shaper queue 7 8000
(config-if)# end
#
```

Web GUI configuration path: **Configuration > QoS > Port Shaping, Port No**.

Figure 8 • **Non-service Queue Shaper**



QoS Egress Port Scheduler and Shapers Port 3 Non-service

Scheduler Mode: Strict Priority

Queue Shaper			
Enable	Rate	Unit	Rate-type
Q7 ☑	8000	kbps	Line
Q6 ☑	4000	kbps	Line

	Enable	Rate	Unit	Rate-type
Port Shaper	□	500	kbps	Line

HQoS Queue Shaper

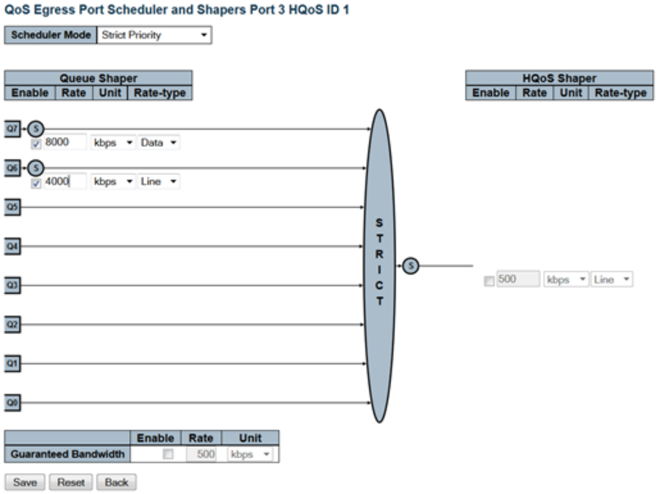
Only queues 6 and 7 have HQoS queue shapers.

The following example lists the commands to enable the HQoS queue level shaper for HQoS ID 1 on queue 6 and queue 7 on port 3, and set the shaping rates to 4000 kbps and 8000 kbps respectively.

```
# configure terminal
! Enable HQoS queue shapers on queues 6 and 7 for HQoS ID 1 on port 3
and set the rate to 4000 kbps for queue 6 and 8000 kbps for queue 7
(config)# hqos 1 queue-shaper queue 6 4000 rate-type data
(config)# hqos 1 queue-shaper queue 7 8000 rate-type data
(config)# end
#
```

Web GUI configuration path: **Configuration > HQoS > HQoS Entries, Configure**.

Figure 9 • **HQoS Queue Shaper**



QoS Egress Port Scheduler and Shapers Port 3 HQoS ID 1

Scheduler Mode	Strict Priority

Queue Shaper

	Enable	Rate	Unit	Rate-type
Q7	☑	8000	kbps	Data
Q6	☑	4000	kbps	Line

HQoS Shaper

Enable	Rate	Unit	Rate-type
□	500	kbps	Line

	Enable	Rate	Unit
Guaranteed Bandwidth	□	500	kbps

Non-service Scheduler

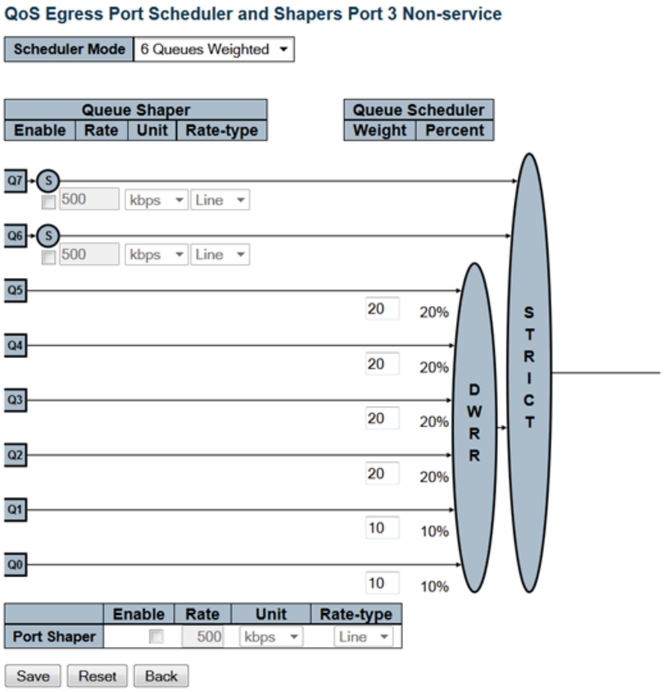
The non-service scheduler is configured using the commands that configure the port scheduler when HQoS is disabled.

The following example lists the commands to set the non-service scheduler mode to 6 Queues Weighted on port 3 with the below weights.

```
Queue 0: 10
Queue 1: 10
Queue 2: 20
Queue 3: 20
Queue 4: 20
Queue 5: 20

# configure terminal
! Set non-service scheduler mode to Weighted on port 3
(config)# interface GigabitEthernet 1/3
(config-if)# qos wrr 10 10 20 20 20 20
(config-if)# end
#
```

Web GUI configuration path: **Configuration > QoS > Port Scheduler, Port No**.

Figure 10 • **Non-service Scheduler**



QoS Egress Port Scheduler and Shapers Port 3 Non-service

Scheduler Mode: 6 Queues Weighted

Queue	Queue Shaper Enable	Rate	Unit	Rate-type	Queue Scheduler Weight	Percent
Q7	□	500	kbps	Line		
Q6	□	500	kbps	Line		
Q5					20	20%
Q4					20	20%
Q3					20	20%
Q2					20	20%
Q1					10	10%
Q0					10	10%

	Enable	Rate	Unit	Rate-type
Port Shaper	□	500	kbps	Line

HQoS Scheduler

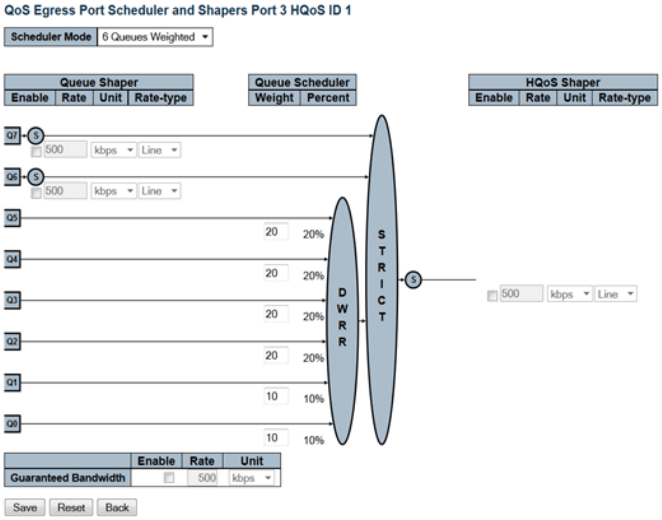
The following example lists the commands to set the HQoS scheduler to 6 Queues Weighted for HQoS ID 1 on port 3 with the below weights:

```
Queue 0: 10
Queue 1: 10
Queue 2: 20
Queue 3: 20
Queue 4: 20
Queue 5: 20
```

```
# configure terminal
! Set HQoS scheduler mode to Weighted for HQoS ID 1 on port 3
(config)# hqos 1 wrr 10 10 20 20 20 20
(config)# end
#
```

Web GUI configuration path: **Configuration > HQoS > HQoS Entries, Configure**

Figure 11 • **HQoS Scheduler**



QoS Egress Port Scheduler and Shapers Port 3 HQoS ID 1

Scheduler Mode: 6 Queues Weighted

Queue	Queue Shaper Enable	Rate	Unit	Rate-type	Queue Scheduler Weight	Percent
Q7	□	500	kbps	Line		
Q6	□	500	kbps	Line		
Q5					20	20%
Q4					20	20%
Q3					20	20%
Q2					20	20%
Q1					10	10%
Q0					10	10%

HQoS Shaper: Enable □ Rate 500 Unit kbps Rate-type Line

	Enable	Rate	Unit
Guaranteed Bandwidth	□	500	kbps

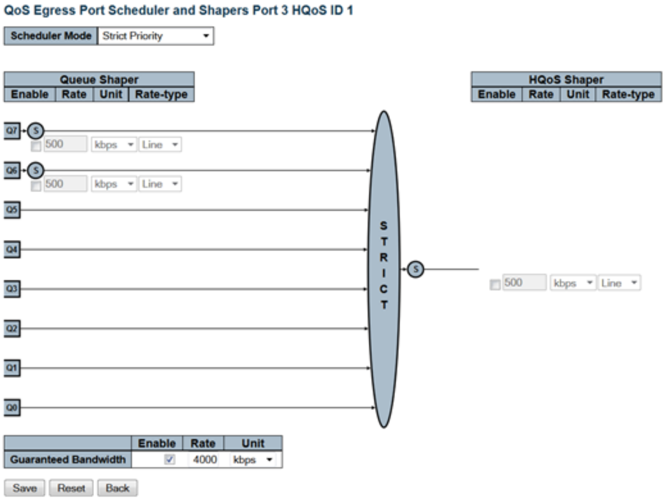
HQoS Guaranteed Bandwidth

The following example lists the commands to enable guaranteed bandwidth for HQoS ID 1 on port 3 and set the rate to 4000 kbps.

```
# configure terminal
! Set the guaranteed bandwidth for HQoS ID 1 on port 3 to 4000 kbps
(config)# hqos 1 guaranteed-bandwidth 4000
(config)# end
#
```

Web GUI configuration path: **Configuration > HQoS > HQoS Entries, Configure**.

Figure 12 • **HQos Guaranteed Bandwidth**



QoS Egress Port Scheduler and Shapers Port 3 HQoS ID 1

Scheduler Mode: Strict Priority

Queue	Queue Shaper Enable	Rate	Unit	Rate-type
Q7	□	500	kbps	Line
Q6	□	500	kbps	Line
Q5				
Q4				
Q3				
Q2				
Q1				
Q0				

HQoS Shaper: Enable □ Rate 500 Unit kbps Rate-type Line

	Enable	Rate	Unit
Guaranteed Bandwidth	☑	4000	kbps

Using RFC2544 Benchmark Tests

This document explains the concept of RFC2544 benchmark test feature. It describes the RFC2544 test profile and test report and shows examples of how to configure and execute the tests using either the ICLI commands or the web GUI.

Cisco ME1200 RFC2544

RFC2544 defines a number of tests that can be used to describe the performance characteristics of a network interconnect device. The purpose is to certify that a service level agreement (SLA) between a customer and a service provider is met. The test frame generation and checking are all done by the switch hardware and software. The following RFC2544 performance tests are supported:

- Throughput – Measure the maximum rate at which at most a certain percentage of frames are lost. Usually set to 0.0%, but configurable.
- Latency – Measure the round-trip time taken by a 1DM frame to exit the traffic generator port and re-enter it. By transmitting more than two 1DM frames in one latency test, it is possible to calculate the delay variation.
- Frame Loss rate – Measure the frame loss at various transmission rates.
- Back-to-Back – Measure the maximum number of frames in a burst with minimum inter-frame gaps the service network can handle without loss of any frame.

In addition, the software includes a test suite tool to create, save, and execute test profiles, and to capture and report results. The following illustration shows the setup that is assumed for the implementation.

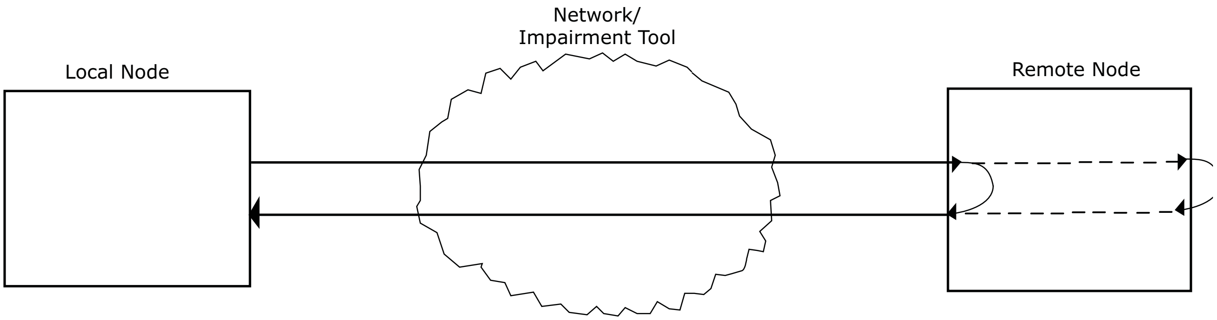


Figure 1 • **Test Setup**

The local node acts as the frame generator and checker, it is the switch running the CEservices software and executing the RFC2544 test.

Note: For RFC2544 to function properly, the remote node must support looping of particular frames. For example, if the remote node is a ME1200 switch, the loop can be created with the `debug rfc2544 loop <port number> enable` command.

RFC2544 Testing

The following ICLI configuration examples for RFC2544 are based on the concepts described in Cisco ME1200 RFC2544, page 14-1.

Create RFC2544 Test Profile

The following steps show how to create or update an RFC2544 profile using the ICLI.

1. Enter configuration mode

```
#configure terminal
```

2. Create an RFC2544 test profile

```
(config) # rfc2544 profile myprofile
```

If a profile named "myprofile" exists, the commands that follow will modify the existing profile instead of creating a new profile.

3. Add a description for the profile

```
(config-rfc2544-profile) # description This is a sample rfc2544 profile
```

4. Configure the egress port on which test frames are generated

```
(config-rfc2544-profile) # test-interface GigabitEthernet 1/1
```

Egress port 1 is used in this case.

5. Configure the DMAC address for the test frames

```
(config-rfc2544-profile) # dmac 00-00-00-00-00-10
```

6. Enable only the throughput test

```
(config-rfc2544-profile) # no latency
```

Throughput and latency are enabled by default, which is why latency needed to be disabled

7. Specify the frame size

```
(config-rfc2544-profile) # frame-size 64
```

8. Enable sequence number checking

```
(config-rfc2544-profile) # sequence-check
```

9. Set the duration of the throughput test to 30 seconds

```
(config-rfc2544-profile) # throughput duration 30
```

10. Set the allowed frame loss to 20%

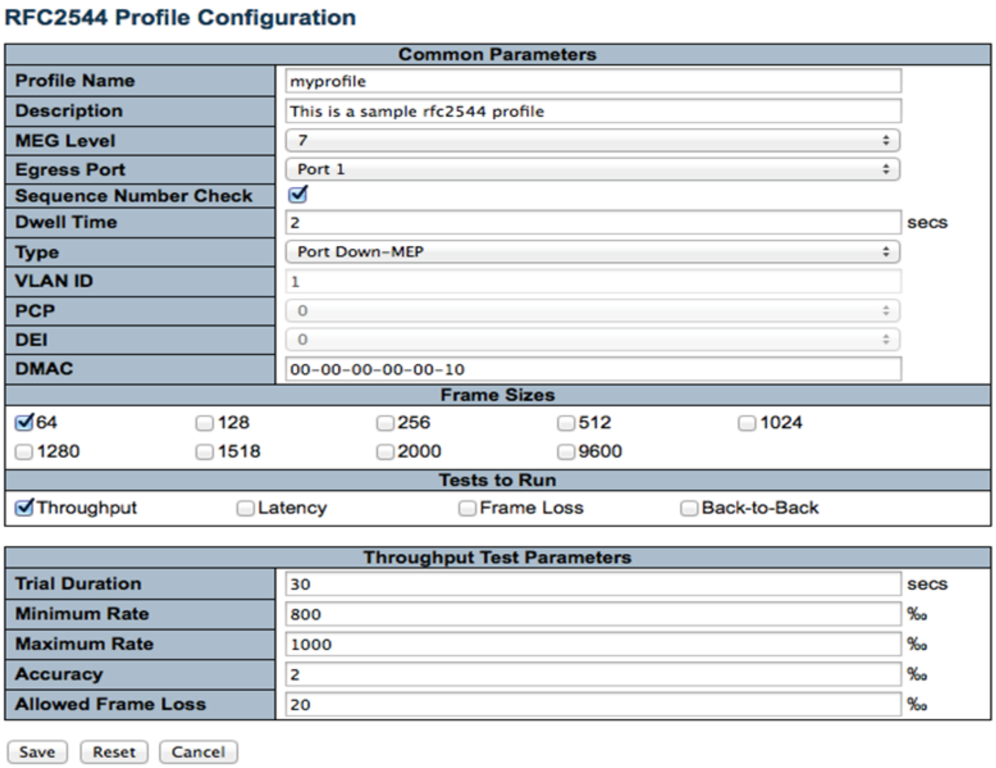
```
(config-rfc2544-profile) # throughput allowed-loss 20
```

11. Finish the profile, leaving all other parameters at their default values

```
(config-rfc2544-profile) # exit
```

The following steps show how to create or update an RFC2544 profile using the web GUI.

Configure the parameters and click **Save** to save the profile.



RFC2544 Profile Configuration

Common Parameters		
Profile Name	myprofile	
Description	This is a sample rfc2544 profile	
MEG Level	7	
Egress Port	Port 1	
Sequence Number Check	☑	
Dwell Time	2	secs
Type	Port Down-MEP	
VLAN ID	1	
PCP	0	
DEI	0	
DMAC	00-00-00-00-00-10	

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	30	secs
Minimum Rate	800	‰
Maximum Rate	1000	‰
Accuracy	2	‰
Allowed Frame Loss	20	‰

Figure 2 • **RFC2544 Profile Configuration**

View RFC2544 Test Profile

The following steps show how to view an RFC2544 profile using the ICLI.

1. Change to exec mode

```
(config) # exec
```

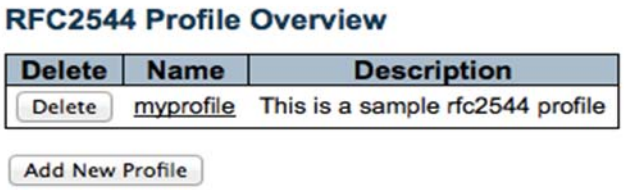
2. Display the profiles saved in the flash

```
# show rfc2544 profile
Profile Name                          Description
--------------------------------  ---------------------------------------
myprofile                             this is a sample profile
```

3. Display the desired profile

```
show rfc2544 profile myprofile
# show rfc2544 profile myprofile
Common configuration:
  Profile name          : myprofile
  Description           : this is a sample profile
  MEG Level             : 7
  Egress interface      : GigabitEthernet 1/1
  Sequence number check : Enabled
  Dwell time            : 2 seconds
  Type                  : Port Down-MEP
  Destination MAC       : 00-00-00-00-00-10
  Source MAC            : 00-01-c1-00-b4-21
  Frame sizes           : 64
  Throughput test       : Enabled
  Latency test          : Disabled
  Frame Loss test       : Disabled
  Back-to-Back test     : Disabled
Throughput configuration:
  Trial duration        : 30 seconds
  Minimum rate          : 800 permille
  Maximum rate          : 1000 permille
  Rate step             : 2 permille
  Allowed frame loss    : 20 permille
#
```

To view or update an RFC2544 profile using the web GUI, click the profile name (myprofile in this case).



RFC2544 Profile Overview

Delete	Name	Description
Delete	myprofile	This is a sample rfc2544 profile

Figure 3 • **Profile List**

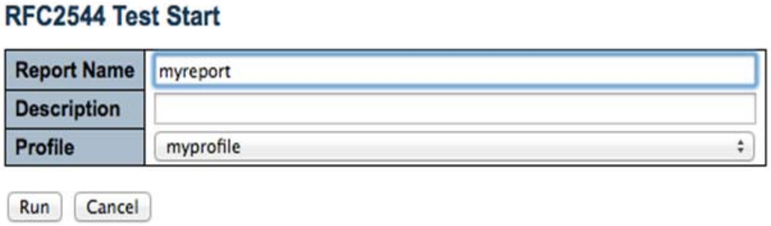
Start RFC2544 Test

To ensure RFC2544 functions properly, the remote node must support looping of the test frames with flipping of DMAC/SMAC of the test frames. If the remote node is a switch, the loop can be enabled by the `debug rfc2544 loop <port number> enable` ICLI command.

An RFC2544 test is triggered by starting the rfc2544 profile and specifying the report name with the following ICLI command.

```
# rfc2544 start myreport profile myprofile
```

An RFC2544 test can also be executed through the web GUI by specifying a report name and selecting the test profile at **RFC2544 > Reports**



RFC2544 Test Start

Report Name	myreport
Description	
Profile	myprofile

Figure 4 • **Report List and Test Execution**

Display RFC2544 Test Report

Display the test reports saved in the flash to determine if the RFC2544 test just triggered is still ongoing.

```
# show rfc2544 report
Report Name             Created                                      Status
```

```
-----------------------------------------------------------------------------
------
myreport              1970-01-02T00:12:49+00:00                  In progress
```

The in progress status indicates the test is ongoing. When the status changes to Succeeded or Failed it means the test has finished and a report has been generated. Use the following ICLI command to display a completed report.

```
# show rfc2544 report myreport
*****************************************************************************
****
* RFC2544 Conformance Test Suite
*****************************************************************************
****
Software configuration:
  Version               : CEServices (standalone) Version 3.40 Build 856563
  Build date            : 2013-10-02T15:30:17+02:00
  Code revision         : bb99cb26bf37Report configuration:
  Report name           : myreport
  Description           :
Overall execution status:
  Started at            : 1970-01-01T22:18:29+00:00
  Ended at              : 1970-01-01T23:26:13+00:00
  Status                : Succeeded
Common configuration:
  Profile name          : myprofile
  Description           : this is an example profile
  MEG Level             : 7
  Egress interface      : GigabitEthernet 1/1
  Sequence number check: Enabled
  Dwell time            : 2 seconds
```

Use the following ICLI command to stop an ongoing test.

```
# rfc2544 stop myreport
```

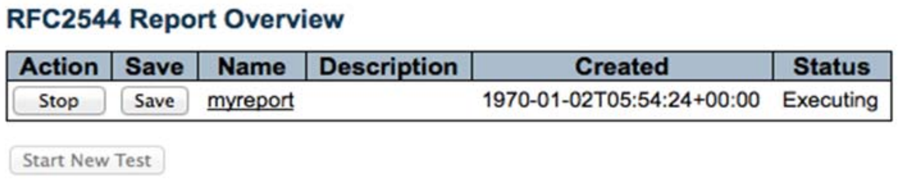
Use the following ICLI command to delete a test report.

```
# rfc2544 delete myreport
```

Use the following ICLI command to save a test report to a TFTP server.

```
# rfc2544 save myreport tftp://server[:port]/path-to-file
```

Test progress can also be monitored through the Web GUI. Click the **Refresh** button at the top-right corner of the **RFC2544 > Reports** page (or check auto-refresh). An ongoing test is shown as executing in the status field.



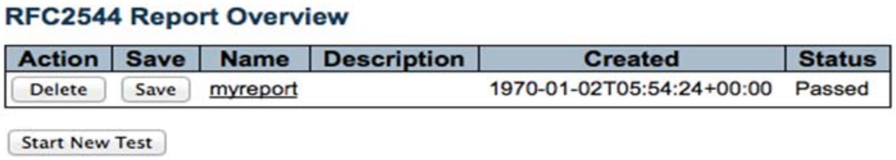
RFC2544 Report Overview

Action	Save	Name	Description	Created	Status
Stop	Save	myreport		1970-01-02T05:54:24+00:00	Executing

Figure 5 • **Ongoing Test**

When a test is executing it can be stopped by clicking **Stop.**

When the test is finished the status changes to either **Passed or Failed.**

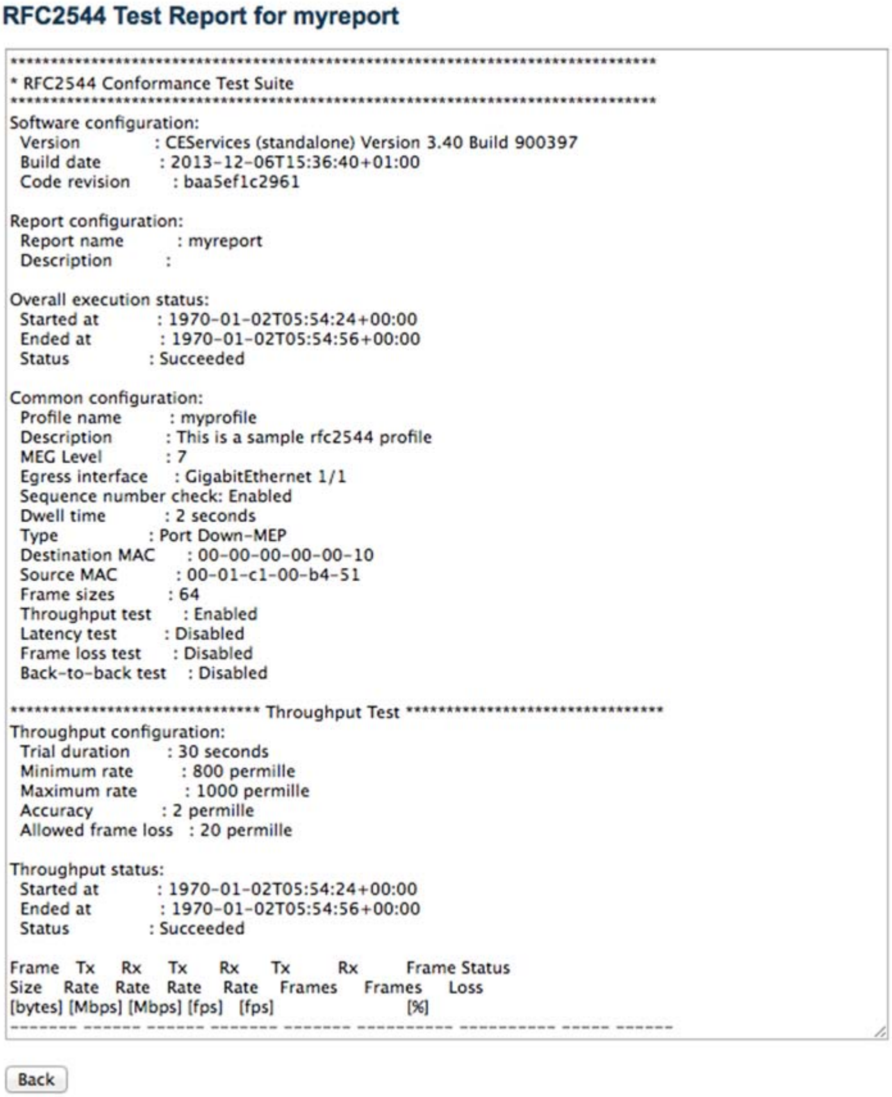


RFC2544 Report Overview

Action	Save	Name	Description	Created	Status
Delete	Save	myreport		1970-01-02T05:54:24+00:00	Passed

Figure 6 **• Completed Test**

Click the report name (myreport in this case) to display a completed report.



RFC2544 Test Report for myreport

```
********************************************************************************
* RFC2544 Conformance Test Suite
********************************************************************************
Software configuration:
  Version             : CEServices (standalone) Version 3.40 Build 900397
  Build date          : 2013-12-06T15:36:40+01:00
  Code revision       : baa5ef1c2961

Report configuration:
  Report name         : myreport
  Description         :

Overall execution status:
  Started at          : 1970-01-02T05:54:24+00:00
  Ended at            : 1970-01-02T05:54:56+00:00
  Status              : Succeeded

Common configuration:
  Profile name        : myprofile
  Description         : This is a sample rfc2544 profile
  MEG Level           : 7
  Egress interface    : GigabitEthernet 1/1
  Sequence number check: Enabled
  Dwell time          : 2 seconds
  Type                : Port Down-MEP
  Destination MAC     : 00-00-00-00-00-10
  Source MAC          : 00-01-c1-00-b4-51
  Frame sizes         : 64
  Throughput test     : Enabled
  Latency test        : Disabled
  Frame loss test     : Disabled
  Back-to-back test   : Disabled

****************************** Throughput Test ********************************
Throughput configuration:
  Trial duration      : 30 seconds
  Minimum rate        : 800 permille
  Maximum rate        : 1000 permille
  Accuracy            : 2 permille
  Allowed frame loss  : 20 permille

Throughput status:
  Started at          : 1970-01-02T05:54:24+00:00
  Ended at            : 1970-01-02T05:54:56+00:00
  Status              : Succeeded

Frame   Tx     Rx     Tx      Rx      Tx         Rx         Frame Status
Size    Rate   Rate   Rate    Rate    Frames     Frames     Loss
[bytes] [Mbps] [Mbps] [fps]   [fps]                         [%]
------- ------ ------ ------- ------- ---------- ---------- ----- ------
```

Figure 7 **• Test Report**

Click **Delete** to delete a test report or **Save** to save it as a text file.

RFC2544 Test Parameters

A test profile must be prepared before an RFC2544 test can be executed. An RFC2544 test profile contains all the parameters associated with one test, where one test may be a combination of one or more sub-tests such as throughput, latency, frame loss, and back-to-back. Up to 16 profiles can be created and saved in the switch flash memory.

The following tables show the common and sub-test specific parameters in a test profile.

Table 1 • **Common Parameters**

Parameter	Description
Profile Name	Each profile must have a name of up to 32 characters. Default: New profile.
Profile Description	Text description up to 128 characters. Default: blank.
MEG Level	MEG level on which the RFC2544 test is run. Default: MEG level 7.
Egress Port	Egress port of the switch on which the RFC2544 test frames are generated and checked.
Sequence Number Check	Option to generate frame sequence number. Default: Disabled.
Dwell Time	Number of seconds wait after each trial before reading statistics from the hardware. Default: 2 seconds.
Type	Type of traffic: Port Down_MEP and VLAN-based Down-MEP. With VLAN-based Down-MEP a configurable VLAN tag will be inserted into the test frames generated.
VLAN ID	VLAN ID if VLAN-based Down_MEP is configured.
PCP	PCP value if VLAN-based Down_MEP is configured.
DEI	DEI value if VLAN-based Down_MEP is configured.
DMAC	DMAC for the generated Port-based or VLAN-based Down-MEP frames.
Frame Size	Frame size for each test: 64,128,256,512,1024,1280,1518,2000, and 9600 bytes. Default: all except 9600.
Sub-tests to run	Sub-test to be run in the profile (Throughput, Latency, Frame Loss, Back-to-Back). Default: Throughput and Latency.

Table 2 • **Throughput Test Parameters**

Parameter	Description
Trial Duration	Duration of trial. Valid range is [1:1800] seconds. Default: 60 seconds.
Minimum and Maximum Rate	Range of rates to search.
Rate Step	Granularity to search within the minimum and maximum rates. All three input parameters are specified in ‰ of the egress port’s actual link speed and in the range [1; 1000] ‰ with a granularity of 1‰. Defaults: Minimum: 800‰ of link speed, Maximum: 1000‰ of link speed, Step size: 20‰ of link speed.
Allowed Frame Loss	Allowable frame loss. Valid range is [0; 100] ‰ with a granularity of 1‰. Default: 0.

Table 3 • **Latency Test Parameters**

Parameter	Description
Trial Duration	Duration of trial. Valid range is [10; 1800] seconds. Default: 120 seconds.
Delay Measurement Interval	Time between each delay measurement. Valid range is [1; 60] seconds in steps of 1 second. Default: 10 seconds.
Allowed Frame Loss	Pass criterion of an allowable frame loss. Valid values must be in range [0; 10%] with a granularity of 0.1%. Default: 0.

Table 4 • **Frame Loss Test Parameters**

Parameter	Description
Trial Duration	Duration of trial. Valid range is [1; 1800] seconds. Default: 60 seconds.
Minimum and Maximum Rate	Range of rates to search.
Rate Step	Granularity to search within the minimum and maximum rates. All three input parameters are specified in ‰ of the egress port’s actual link speed and in the range [1; 1000] ‰ with a granularity of 1‰. Defaults: Minimum: 800‰ of link speed, Maximum: 1000‰ of link speed, Step size: 20‰ of link speed.

Table 5 • **Back-to-Back Test Parameters**

Parameter	Description
Trial Duration	Duration of burst. Valid range is [100; 10000] milliseconds. Default: 2000 milliseconds.
Trial Count	Number of times the trial is executed. Valid range is [1; 100]. Default: 50.

RFC2544 Test Report

An RFC2544 test report is generated after an RFC2544 test profile has been executed. The test report is in clear text format and contains all the input parameters defined by the associated test profile as well as all the measurement results. The test report is used to certify that an SLA is met or not.

The last 10 test reports are kept in the flash memory of the switch. They can be viewed through CLI or downloaded to a PC through TFTP.

The following is an example of a test report named myreport, which has been generated after the myprofile test profile was executed.

General Information

The first part of the test report lists the general information of the software version, test report name, execution date/time, and status. It also lists the associated test profile information with all the common configuration parameters of that test profile.

```
****************************************************************************
****
* RFC2544 Conformance Test Suite
****************************************************************************
****
Software configuration:
  Version              : CEServices (standalone) Version 3.40 Build 856563
  Build date           : 2013-10-02T15:30:17+02:00
  Code revision        : bb99cb26bf37
```

```
Report configuration:
  Report name          : myreport
  Description          :
Overall execution status:
  Started at           : 1970-01-01T22:18:29+00:00
  Ended at             : 1970-01-01T23:26:13+00:00
  Status               : Succeeded
Common configuration:
  Profile name         : myprofile
  Description          : enable all sub-tests
  MEG Level            : 7
  Egress interface     : GigabitEthernet 1/1
  Sequence number check: Enabled
  Dwell time           : 2 seconds
  Type                 : Port Down-MEP
  Destination MAC      : 00-00-00-00-00-04
  Source MAC           : 00-01-c1-00-b4-21
  Frame sizes          : 64 128 256 512 1024 1280 1518 2000
  Throughput test      : Enabled
  Latency test         : Enabled
  Frame loss test      : Enabled
  Back-to-back test    : Enabled
```

Configuration and Test Results

The general information is followed by the configurations and test results of each RFC2544 sub-test.

Throughput Text

The test report for the throughput sub-test lists the configuration parameters for the throughput test and the execution date/time and status. Each row is the measurement result of each throughput test trial for a special frame size enabled through the test profile. The listed values include measured throughput, frame sending the receiving rates, number of frames sent and received for each trial, and frame loss rate.

```
******************************* Throughput Test
********************************
Throughput configuration:
  Trial duration       : 60 seconds
  Minimum rate         : 800 permille
  Maximum rate         : 1000 permille
  Rate step            : 2 permille
  Allowed frame loss   : 0 permille
Throughput status:
  Started at           : 1970-01-01T22:18:29+00:00
  Ended at             : 1970-01-01T22:26:45+00:00
  Status               : Succeeded
Frame   Tx     Rx     Tx      Rx      Tx         Rx         Frame Status
Size    Rate   Rate   Rate    Rate    Frames     Frames     Loss
[bytes] [Mbps] [Mbps] [fps]   [fps]                         [%]
------- ------ ------ ------- ------- ---------- ---------- ----- ------
     64  999.9  999.9 1488071 1488071   89284314   89284314   0.0 PASS
    128  999.9  999.9  844582  844582   50674931   50674931   0.0 PASS
    256  999.9  999.9  452890  452890   27173438   27173438   0.0 PASS
    512  999.9  999.9  234958  234958   14097494   14097494   0.0 PASS
   1024  999.9  999.9  119729  119729    7183797    7183797   0.0 PASS
   1280  999.9  999.9   96152   96152    5769124    5769124   0.0 PASS
   1518  999.9  999.9   81272   81272    4876358    4876358   0.0 PASS
   2000  999.9  999.9   61879   61879    3712768    3712768   0.0 PASS
```

Latency Test

The test report for the latency sub-test lists the configuration parameters for the latency test and the execution date/time and status. Each row lists the measured delay and delay variation with a special frame size enabled through the test profile. It also lists the frame sending rate, number of frames sent and received for each trial.

```
********************************* Latency Test
*********************************
Latency configuration:
  Trial duration       : 120 seconds
  Delay meas. interval : 10 seconds
  Allowed frame loss   : 0 permille
Latency status:
  Started at           : 1970-01-01T22:26:45+00:00
  Ended at             : 1970-01-01T22:43:01+00:00
  Status               : Succeeded
Frame   Tx     Tx         Rx         Min/Avg/Max      Min/Avg/Max       Status
Size    Rate   Frames      Frames     Delay             Delay Var.
[bytes] [Mbps]                        [usecs]           [usecs]
------- ------ ---------- ---------- ----------------- -----------------
------
     64  999.7  178532323  178532323             3/3/3             0/0/0 PASS
    128  999.7  101329475  101329475             3/3/3             0/0/0 PASS
    256  999.7   54336108   54336108             4/4/4             0/0/0 PASS
    512  999.7   28189582   28189582             6/6/6             0/0/0 PASS
   1024  999.7   14364885   14364885          10/10/10             0/0/0 PASS
   1280  999.7   11536065   11536065          12/12/12             0/0/0 PASS
   1518  999.7    9750940    9750940          14/14/14             0/0/0 PASS
   2000  999.7    7424184    7424184          13/18/18             0/0/5 PASS
```

Frame Loss Test

The test report for the frame loss sub-test lists the configuration parameters for the frame loss test and the execution date/time and status. Each row lists the frame loss rate with a special frame size enabled through the test profile. It also lists the frame sending and receiving rates, number of frames sent and received for each trial.

```
******************************* Frame Loss Test
*******************************
Frame loss configuration:
  Trial duration       : 60 seconds
  Minimum rate         : 800 permille
  Maximum rate         : 1000 permille
  Rate step            : 5 permille
Frame Loss status:
  Started at           : 1970-01-01T22:43:01+00:00
  Ended at             : 1970-01-01T22:59:33+00:00
  Status               : Succeeded
Frame   Tx     Rx     Tx      Rx      Tx         Rx         Frame Status
Size    Rate   Rate   Rate    Rate    Frames     Frames     Loss
[bytes] [Mbps] [Mbps] [fps]   [fps]                         [%]
------- ------ ------ ------- ------- ---------- ---------- ----- ------
     64  999.9  999.9 1488064 1488064   89283848   89283848   0.0 PASS
     64  994.9  994.9 1480630 1480630   88837833   88837833   0.0 PASS
```

```
    128  999.9  999.9  844581  844581   50674865   50674865   0.0 PASS
    128  994.9  994.9  840361  840361   50421665   50421665   0.0 PASS
    256  999.9  999.9  452890  452890   27173435   27173435   0.0 PASS\
    256  994.9  994.9  450629  450629   27037742   27037742   0.0 PASS
    512  999.9  999.9  234958  234958   14097535   14097535   0.0 PASS
    512  994.9  994.9  233786  233786   14027162   14027162   0.0 PASS
   1024  999.9  999.9  119729  119729    7183796    7183796   0.0 PASS
   1024  994.9  994.9  119133  119133    7148017    7148017   0.0 PASS
   1280  999.9  999.9   96152   96152    5769126    5769126   0.0 PASS
   1280  994.9  994.9   95672   95672    5740378    5740378   0.0 PASS
   1518  999.9  999.9   81272   81272    4876360    4876360   0.0 PASS
   1518  994.9  994.9   80867   80867    4852071    4852071   0.0 PASS
   2000  999.9  999.9   61879   61879    3712772    3712772   0.0 PASS
   2000  994.9  994.9   61571   61571    3694279    3694279   0.0 PASS
```

Back-to-Back Test

The test report for the back-to-back sub-test lists the configuration parameters for the back-to-back test and the execution date/time and status. Each row lists the maximum number of frames in a burst with minimum inter-frame gaps that the remote node can handle without loss of any frame with specific frame size enabled through the test profile. It also lists the frame sending and receiving rates for each trial.

```
****************************** Back-to-back Test
*******************************
Back-to-back configuration:
  Trial duration       : 2000 milliseconds
  Trial count          : 50
Back-to-back status:
  Started at           : 1970-01-01T22:59:33+00:00
  Ended at             : 1970-01-01T23:26:13+00:00
  Status               : Succeeded
Frame   Tx     Rx     Tx      Rx      Tx         Rx         Frame Status
Size    Rate   Rate   Rate    Rate    Frames     Frames     Loss
[bytes] [Mbps] [Mbps] [fps]   [fps]                         [%]
------- ------ ------ ------- ------- ---------- ---------- ----- ------
     64  999.3  999.3 1487095 1487095    2974191    2974191   0.0 PASS
     64  999.3  999.3 1487118 1487118    2974236    2974236   0.0 PASS
     64  999.3  999.3 1487122 1487122    2974245    2974245   0.0 PASS
     64  999.3  999.3 1487060 1487060    2974121    2974121   0.0 PASS
     64  999.3  999.3 1487114 1487114    2974229    2974229   0.0 PASS
     64  999.3  999.3 1487124 1487124    2974249    2974249   0.0 PASS
     64  999.3  999.3 1487126 1487126    2974253    2974253   0.0 PASS
     64  999.3  999.3 1487122 1487122    2974244    2974244   0.0 PASS
```

Test Date and Time

At the end of the test report provides the information of the date/time when the test profile has been finished execution and the overall result of the test.

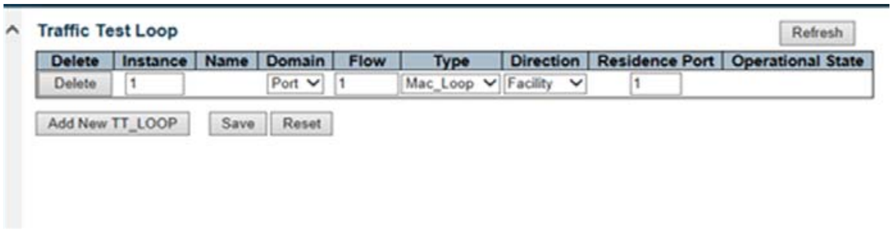
```
******************************** Overall Result
********************************
  Ended at             : 1970-01-01T23:26:13+00:00
  Status               : Succeeded
```

Configuring Traffic Test Loop

The following steps show how to configure a traffic test loop using the web interface.

1. Display traffic test loop information.

Configuration > Traffic Test > Loop



Traffic Test Loop

Delete	Instance	Name	Domain	Flow	Type	Direction	Residence Port	Operational State
Delete	1		Port	1	Mac_Loop	Facility	1	

Figure 8 **• Traffic Test Loop Configuration Page**

2. Create new traffic test loop.

Click **Add New TT_LOOP** and provide values for the following parameters.

Parameter	Description
Instance	ID of the new TT_LOOP. Once a TT_LOOP is created the parameters of that TT_LOOP can be modified by clicking the ID.
Name	Name of the instance.
Domain	Port: Loop in the Port domain. EVC: Loop in the EVC domain. Flow is an EVC. The EVC must have been created already. VLAN: Loop in the VLAN domain. Flow is a VLAN. The VLAN must have been created already for an Up-TT-LOOP.
Flow	Port number for port domain, EVC ID for EVC domain, and VLAN ID for VLAN domain.
Type	Mac_loop: All frames in the flow are looped with SMAC and DMAC swap. OAM_loop: Loop LBM to LBR and DMM to DMR (currently not supported).
Direction	Facility loop: Looping is done from ingress to egress. Terminal loop: Looping is done from egress to ingress (currently not supported).
Residence Port	Port where the TT_LOOP is resident. For an EVC loop the port must be a port in the EVC. For a VLAN loop the port must be a VLAN member.

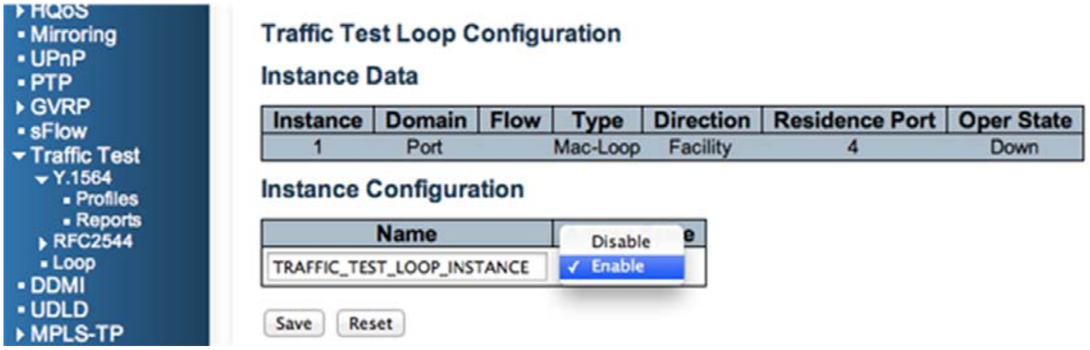
3. Display loop instance.

Click the loop instance number to display the **Traffic Loop Administration** configuration settings.

Note: After a TT_LOOP instance is created it’s operational status will still be DOWN, unless all the resources are available for that loop instance and also the administration state of the loop instance is set to Enabled.

4. Enable loop instance.

Select **Enable**.



Traffic Test Loop Configuration

Instance Data

Instance	Domain	Flow	Type	Direction	Residence Port	Oper State
1	Port		Mac-Loop	Facility	4	Down

Instance Configuration

Name	e
TRAFFIC_TEST_LOOP_INSTANCE	Disable ✓ Enable

Figure 9 **• Enable Traffic Test Loop Instance**

The following code creates a MAC swapping loop on port 4 in the port domain with operational state UP using the ICLI interface.

```
(config)# traffic-test-loop 1 type mac-loop interface GigabitEthernet 1/4
direction facility domain port level 0
```

Loop domain EVC or VLAN can be used to avoid service interrupting other services on the same physical port. The loop domain port is used for the configuration, which eliminates dependency of EVC and VLAN settings of the switch when the service interruption is not a concern. The following TT_LOOP combinations are supported:

- Facility mac_swap loop in PORT domain
- Facility mac_swap loop in EVC domain
- Facilty OAM loop in EVC domain
- Terminal OAM loop in EVC domain

Because Y.2544 tests are port based a TT_LOOP instance of MAC swapping on a port domain should be configured.

Software Configuration Y.1564

This document describes the Y.1564 test feature supported by Cisco ME1200. It explains Y.1564 test profile and test report, and gives examples on how to configure and execute Y.1564 test through Web GUI or CLI interface.

Understanding ITU-T Y.1564

ITU-T Y.1564 (sometimes called EtherSAM – Ethernet Service Activation Methodology) is a QoS and network performance ITU-T Ethernet-based service test methodology. This out-of-service testing procedure tests service turn-up, installation, and troubleshooting of Ethernet-based services with the goal of assuring and verifying committed service level agreement (SLA) performances.

Prior to Y.1564 the most widely used testing tool to assess performance of Ethernet-based services was IETF RFC 2544 (RFC 2544 test is also supported by ME1200. For more information, see “Using RFC2544 Benchmark Tests”), which was created to evaluate the performance characteristics of network devices in a lab. It includes throughput, burstability (back-to-back test), frame loss, and latency tests, and is used in Ethernet networks globally. However it does not include all required measurements such as packet delay variation, QoS measurement with bandwidth profiles (CIR, CBS, EIR, EBS, and color mode), and multiple concurrent service levels. Contrary to RFC2544, Y.1564 allows simultaneous testing of multiple Ethernet services and measures if they qualify to the committed SLA attributes. It also validates the different QoS mechanisms provisioned in the network to prioritize the different service types, allowing service providers faster deployment and easier service and network troubleshooting.

Y.1564 defines test streams (or flows) with service attributes aligned to the Metro Ethernet Forum (MEF) 10.2 definitions. These test flows can be classified using various mechanisms such as 802.1q VLAN, 802.1ad, DSCP, and class of service (CoS) profiles. These services are defined at the UNI level with different frame and bandwidth profiles such as the service’s maximum transmission unit (MTU) or frame size, committed information rate (CIR), and excess information rate (EIR) in single test.

Y.1564 is carrier Ethernet switch feature built on both hardware and software. The test flows are generated and injected by the switch’s hardware based frame generation engine at UNI ingress at one end of an EVC and monitored by the OAM Processor at the UNI egress at the other end of the EVC. Nanosecond accurate delay measurement is made possible with the hardware based time stamp engine.

Y.1564 Test Types

Y.1564 test methodology has the following two main objectives.

- Validate that each Ethernet-based service is correctly configured.
- Validate the quality of the services as delivered to the end-user.

Accordingly, the methodology comprises service configuration test and a service performance test as shown in the following figure.

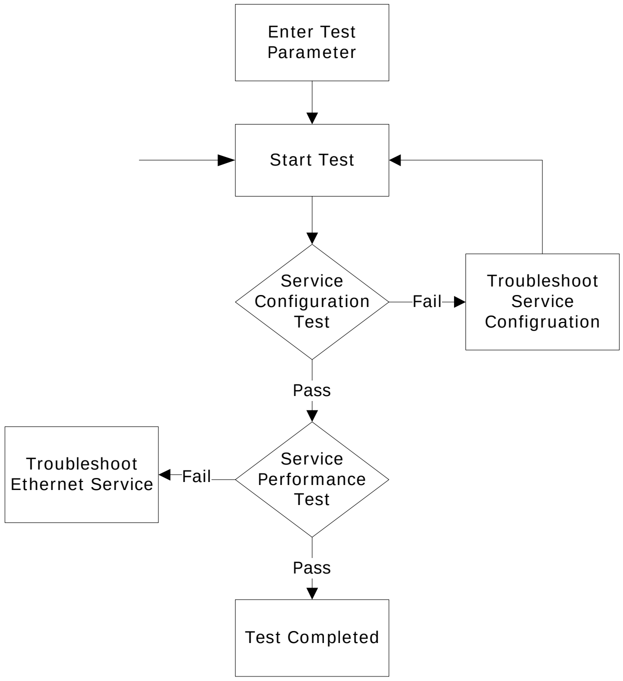

Enter Test Parameter
Start Test
Service Configuration Test
Fail
Troubleshoot Service Configruation
Pass
Troubleshoot Ethernet Service
Fail
Service Performance Test
Pass
Test Completed

***Figure 1* • Service Activation Methodology**

The goal of the service configuration test is to validate that the services are configured as intended. Service configuration test comprises of CIR, EIR, and traffic policing tests. The following sections describe these tests, along with the service performance test.

CIR Configuration Test

Step load is normally used for the CIR test to gradually reach the CIR. When step count is 4 (default), a test flow will transmit at 25% of CIR at SRC. Measure the received IR, FLR, FTD, and FDV. FLRsac is the frame loss ratio limit as specified in the SAC (service acceptance criteria). If the FLR (including errored frames), FTD, and FDV are all within the limits specified by the SAC, increase transmitted IR and repeat the test (at 50%, 75%, and 100% of CIR) or other steps as configured by the user. If 100% of the CIR has been reached successfully within the SAC limits, then the result is PASS.

EIR Configuration Test

For color aware test, transmit frames marked green and yellow into the measurement point at a rate equal to CIR for the green frames and EIR for the yellow frames. Measure the received rate: IR-G for green frames, IR-Y for yellow frames, and IR-T for the total combined rate. Also measure FLR-G frame loss ratio of green frame, FTD-G frame transfer delay of the green frame, FDV-G frame delay variation of the green frames. If FLR-G, FTD-G, and FDV-G are all within the SAC limits then the result is PASS.

For non-color-aware test, transmit at an IR equal to CIR + EIR and measure the received IR-T. Also measure FLR, FTD, and FDV. If CIR x (1-FLRsac) ? IR-T ? CIR + EIR, then the results is PASS.

Traffic Policing Test

For color aware test, transmit green marked frames at the source at an information rate equal to CIR and transmit yellow marked frames at an information rate of 125% EIR. Measure the received IR. Measure IR-G (green frames), IR-Y (yellow frames), IR-T (total frames). Also measure FLR-G, FTD-G, and FDV-G. If FLR-G, FTD-G, and FDV-G are all within the SAC limits, and if IR-T ? CIR + EIR + M (M for the effect of the traffic policer's CBS and EBS settings), then the result is PASS.

For non-color-aware test, transmit at the source with an IR equal to CIR + 125%EIR, measure the IR, FLR, FTD, and FDV. If CIR x (1-FLRsac) ? IR-T ? CIR + EIR + M (M for the effect of the traffic policer's CBS and EBS settings), then the result is PASS.

Service Performance Test

Service performance test validates the quality of the services over time up to 24 hours. All services must transmit green marked frames of an IR equal to CIR. Measure the received IR, FLR, FTD, FDV, and Service Availability. The services must operate at or above the SAC performance levels for the service to be accepted.

Y.1564 Test Profile

A test profile is needed to execute a Y.1564 test. A Y.1564 test profile contains all the parameters associated with one test, which may be a combination of one or more of sub-tests (configuration test includes CIR, EIR and traffic policing test, and performance test).

Previously saved Y.1564 test profiles are listed on the Y.1564 Profiles Overview web GUI page (Configuration > Traffic Test > Y.1564 > Profiles). Clicking the profile name displays the contents of any existing test profile. Click the delete button to delete a test profile.

Click Add New Profile to create a new profile in the profile configuration page where you configure all the parameters for the new test profile. Up to 16 test profiles can be created and saved in the flash memory of the switch.

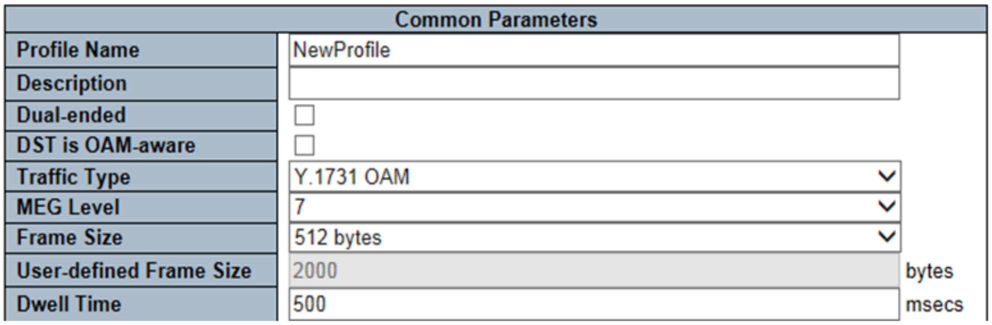
Existing profiles can also be shown with the following iCLI command.

```
# show y1564 profile
```

And new profile can be created by the following iCLI commands.

```
! Get into configuration mode
# configure terminal
! Create a Y.1564 test profile and name it “MyProfile”.
! If a profile named “MyProfile” already exists, The command that follows will
! modify the existing profile instead of creating a new profile.
(config)# y1564 profile MyProfile
(configure-y1564-profile)#
```

The following illustration shows the common parameters and sub-test specific parameters in a test profile.



Common Parameters		
Profile Name	NewProfile	
Description		
Dual-ended	□	
DST is OAM-aware	□	
Traffic Type	Y.1731 OAM	
MEG Level	7	
Frame Size	512 bytes	
User-defined Frame Size	2000	bytes
Dwell Time	500	msecs

Figure 2 • **Common Parameters**

The following table describes the common parameters.

***Table 1* • Common Parameters**

Parameter	Description	Comments
Profile Name	Each profile must have a unique name of up to 32 characters.	Default: NewProfile
Description	Up to 128 character description associated with the profile.	Default: blank
Dual-ended	When checked, test flows are generated at SRC and statistics are gathered at DST. Test traffic only travels the network once. This requires a network management station (NMS) to control traffic, gather results, and create a test report. Currently, only single ended tests are supported: SRC transmits traffic and expects a looped version to return at the NNI where it egressed, but with DMAC and SMAC swapped.	Default: unchecked
DST is OAM-aware	When checked, this switch transmits Y.1731 LBM frames as background traffic, and expects the remote end to return Y.1731 LBR frames. When unchecked, this switch transmits Y.1731 TST frames as background traffic, and expects the remote end to loop this traffic while swapping DMAC and SMAC only. For delay measurements, this switch transmits Y.1731 DMM frames if destination is OAM-aware and Y.1731 1DM frames if destination is OAM-unaware.	Default: unchecked
Traffic Type	When set to Y.1731 OAM it means that Y.1731 OAM frame will be used as background traffic. When set to Simulated Customer Traffic software will build up one or two frames (green/yellow) that it knows will be caught by a particular ECE. Up to 8 ECEs may be tested simultaneously.	Default: Y.1731 OAM
MEG Level	MEG level on which the Y.1564 test is run.	Default: MEG level 7
Frame Size	Frame size for each test.	Default: 512 Bytes

Table 1 • **Common Parameters (continued)**

Parameter	Description	Comments
User-defined Frame Size	Programmable frame size when User-defined Frame size is the selected.	Default: 2000 Bytes
Dwell Time	Milliseconds to wait after each trial for the test to settle before reading statistics from the hardware.	Default: 500

The following iCLI commands show and example configuration.

```
! edit the y1564 test profile named “myprofile”
(config)# y1564 profile MyProfile
! add a description to the profile
(config-y1564-profile)# description This is a sample description
! set traffic type to y.1731 OAM frames instead of simulated customer traffic
(config-y1564-profile)# traffic-type oam
! set destination to be oam aware so that Y.1731 LBM and DMM frames will be used
(config-y1564-profile)# dst-oam-aware
! set MEG level
(config-y1564-profile)# meg-level 7
! set dwell time to be 500 ms
(config-y1564-profile)# dwell-time 500
! set test frame size to be user defined
(config-y1564-profile)# emix u
! set user defined frame size to be 1000 bytes
(config-y1564-profile)# user-defined-frame-size 1000
```

Service Acceptance Criteria

Service Acceptance Criteria (SAC) are used to ensure that the service meets its functionality and quality requirements, and that the service provider is ready to operate the new service when it has been deployed. The SAC is also used as the PASS criteria for each of the Y.1564 sub-tests.

1. Acceptable FLR – the maximum acceptable frame loss rate in the range [1; 1000] ‰.

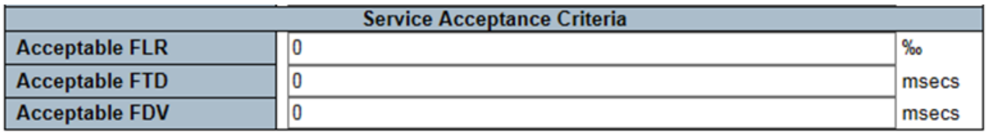
The number is used for each of the enabled sub tests. If the policer belonging to the ECE under test is non-color-aware and the test is injecting traffic above CIR (which can occur in the EIR configuration and the traffic policing tests), method 1 is used when calculating the PASS/FAIL criterion. Otherwise method 2 is used.

- Method 1: The expected total Rx frame count is computed based on the policer rate and the duration of the trial. If the actual Rx frame count is less than the expected minus the acceptable frame loss set with this parameter, the test fails. Otherwise it succeeds.
- Method 2: The actual frame drop is computed as the Tx count minus the Rx count. If this number exceeds the acceptable frame drop (computed from this parameter), the test fails. Otherwise it succeeds.

Method 2 cannot always be used because only green frames are transmitted for non-color-aware tests, and because injection occurs above CIR, frames may get dropped, so that method 1 (which doesn't use the actual Tx frame count) must be used.

2. Acceptable FTD – the maximum transfer delay in milliseconds.

3. Acceptable FDV – the maximum delay variation in milliseconds.



Service Acceptance Criteria		
Acceptable FLR	0	‰
Acceptable FTD	0	msecs
Acceptable FDV	0	msecs

Figure 3 • **Service Acceptance Criteria**

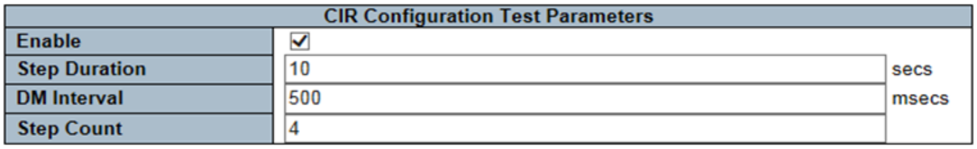
The following iCLI commands can be used to enter SAC parameters.

```
! set frame delay vriation to be 100 ms
(config-y1564-profile)# acceptable-fdv 100
!set frame loss ratio to be 50 ‰
(config-y1564-profile)# acceptable-flr 50
? set frame transfer delay to be 200 ms
(config-y1564-profile)# acceptable-ftd 200
```

CIR Configuration Test Parameters

For this test frames are sent at a rate equal to CIR with configured frame size and duration. Received IR, FLR, FTD, and FDV are measured and compared against the SAC limits. If FLR, FTD, and FDV are all within the SAC limits, then the result is PASS.

1. Enable – enable CIR configuration test
2. Step duration – number of seconds each step will run. Default: 10 seconds.
3. Delay measurement interval – number of milliseconds between each delay measurement. Default: 500 milliseconds.
4. Step count – number of steps for step load CIR test.



CIR Configuration Test Parameters		
Enable	☑	
Step Duration	10	secs
DM Interval	500	msecs
Step Count	4	

Figure 4 • **CIR Configuration Test Parameters**

The following iCL commands enable a CIR test with dwell time of 400 ms, step duration of 10 s, and five steps.

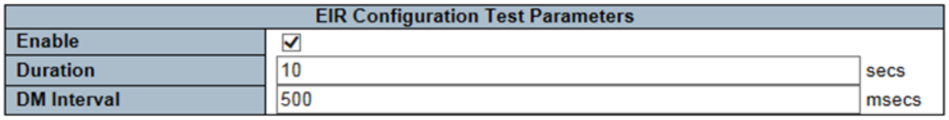
```
(config-y1564-profile)# cir-test dm-interval 400 duration 10 step-count 5
```

EIR Configuration Test Parameters

For this test frames are sent at a rate equal to CIR for the green frames and EIR for the yellow frames with configured frame size and duration. Received IR, FLR, FTD, and FDV are measured and compared against the SAC limits. If FLR-green, FTD-green, and FDV-green are all within the SAC limits, then the result is PASS.

1. Enable – enable EIR configuration test
2. Duration – number of seconds the test will run. Default: 10 seconds.

3. Delay measurement interval – number of milliseconds between each delay measurement. Default: 500 milliseconds.



EIR Configuration Test Parameters		
Enable	☑	
Duration	10	secs
DM Interval	500	msecs

Figure 5 • **EIR Configuration Test Parameters**

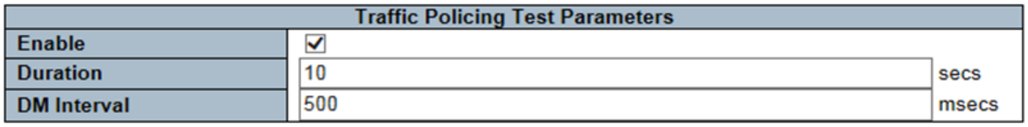
The following iCLI commands enable an EIR test with dwell time of 400 ms with a step duration of 10 s.

```
(config-y1564-profile)# eir-test dm-interval 400 duration 10
```

Traffic Policing Test Parameters

For this test frames are sent at a rate equal to CIR for the green frames and 125% x EIR for the yellow frames with configured frame size and duration. Received IR, FLR, FTD, and FDV are measured and compared against the SAC limits. If FLR-green, FTD-green, and FDV-green are all within the SAC limits, and if IR-T ? CIR + EIR + M, then the result is PASS.

1. Enable – enable EIR configuration test
2. Duration – number of seconds the test will run. Default: 10 seconds.
3. Delay measurement interval – number of milliseconds between each delay measurement. Default: 500 milliseconds.



Traffic Policing Test Parameters		
Enable	☑	
Duration	10	secs
DM Interval	500	msecs

Figure 6 • **Traffic Policing Test Parameters**

The following ICLI commands enable a traffic policing test with dwell time of 400 ms and a step duration of 10 s.

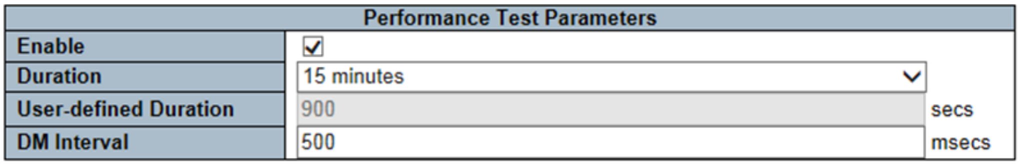
```
(config-y1564-profile)# traffic-policing-test dm-interval 400 duration 10
```

Performance Test Parameters

The service performance test validates the quality of the services over time. All services are generated at once to their configured CIR with configured frame size and duration. Received IR, FLR, FTD, FDV, and AVAIL are measured simultaneously.

1. Enable – enable performance Test
2. Duration – number of seconds the performance test will run. Supported durations: 15 minutes, 2 hours, 24 hours, and user-defined. Default: 15 mimutes.
3. User-defined duration – user-defined test duration in seconds if user-defined duration mode is selected. Default: 900seconds

4. Delay measurement interval – number of milliseconds between each delay measurement. Default: 500 milliseconds.



Performance Test Parameters		
Enable	☑	
Duration	15 minutes	
User-defined Duration	900	secs
DM Interval	500	msecs

Figure 7 • **Performance Test Parameters**

The following iCLI commands enable a performance test with dwell time of 400 ms and a step duration of 2 hours.

```
(config-y1564-profile)# performance-test dm-interval 400 duration 7200
(config-y1564-profile)# exit
(config)#exit
#
```

The show command displays the configured text profile.

```
#show y1564 profile myprofile
Profile configuration:
    Profile name        :myprofile
    Description            :This is a sample profile
    Measurement type    :Single-ended (DST loops traffic)
    DST is OAM aware    :No
Backgroup traffic type :Y.1731 TST    Y.1731 LBM
Delay measurement type : Y.1731 1DM   Y.1731 DMM
MEG level            : 7
Frame size            : user-defined(EMIX= u)
User-defined frame size :1000 bytes
CIR configuration test : Enabled
EIR configuration test : Enabled
Traffic policing test :Enabled
Service performance test: Enabled
Acceptable FLR: 50 permille
Acceptable FTD:200msecs
Acceptable FDV:100msecs
Configuration:
Duration per step  : 10 seconds
Delay meas. Interval : 400msecs
Step count: 5
Configuration:
Duration              : 10 seconds
Delay meas. Interval : 400msecs
Configuration:
Duration              : 10 seconds
Delay meas. Interval : 400msecs
Configuration:
Duration              : 7200 seconds
Delay meas. Interval : 400msecs
```

Y.1564 Test and Test Report

A new Y.1564 test report is generated and saved after each Y.1564 test. Test reports are listed on the Y.1564 Report Overview page of the web GUI (Configuration > Traffic Test > Y.1564 > Reports). The contents of a test report can be viewed by clicking the report name. A test report can be deleted when no longer needed by clicking the delete button.

The following iCLI command can also be use to display a test report. Append the report name to display the content of a specific test report.

```
# show y1564 report
```

Test Start

Use the Y.1564 Test Start page to specify the following:

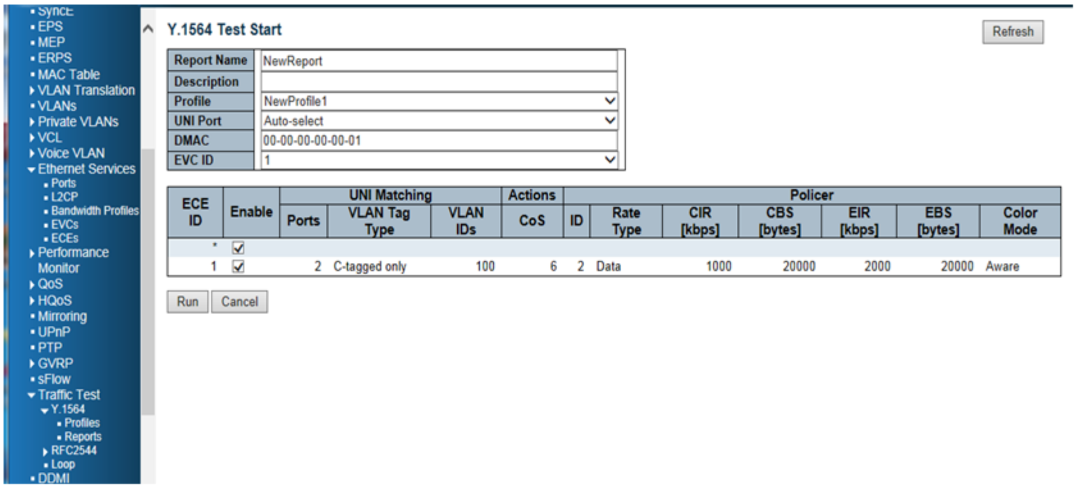
1. File name of the test report, Default: NewReport;
2. Description for the test : Default : blank;
3. Y.1564 test profile (created and saved as described in the previous chapter. Default : the first saved test profile;
4. UNI Port on which the Y.1564 test will be executed, Default : Auto-select (the lowest numbered UNI port of the selected EVC);
5. DMAC of the test flows, Default : 00-00-00-00-00-01;
6. EVC on which the Y.1564 will be executed. Default: the lowest configured EVC ID

Y.1564 test works by defining test flows match service attributes of the EVC (or CoS per EVC) under test. The service attributes needed for generating Y.1564 test flows can be automatically derived from the EVC configuration data because Y.1564 is an embedded feature on ME1200 where all the Ethernet services are configured and saved.

Once the EVC ID has been selected, a table of ECE entries associated with that EVC will be displayed. ECE entries are configured and saved during the creation of an EVC, and ECEs are used to store the UNI related service attributes for that EVC. For more information, see “MEF Service Configuration.” One or more ECEs may map to a single EVC with each ECE corresponding to a different CoS with different bandwidth profile. One Y.1564 test flow must be generated and measured for each ECE of an EVC. Currently, only one Y.1564 test flow can be supported at each test so the user needs to select only one ECE in the ECE table each time.

Since dual-ended Y.1564 test is not supported yet with the current software release so a logical loopback must be configured at the remote location equipment before the user can click “Start New Test” button to start a y.1564 test. Refer to the configuration guide of traffic test loop at the end of the document.

Through WEB GUI click Start New Test to display the Y.1564 Test Start page for preparing a new Y.1564 test.



Y.1564 Test Start

Report Name	NewReport
Description	
Profile	NewProfile1
UNI Port	Auto-select
DMAC	00-00-00-00-00-01
EVC ID	1

ECE ID	Enable	UNI Matching			Actions	Policer						
		Ports	VLAN Tag Type	VLAN IDs	CoS	ID	Rate Type	CIR [kbps]	CBS [bytes]	EIR [kbps]	EBS [bytes]	Color Mode
*	☑											
1	☑	2	C-tagged only	100	6	2	Data	1000	20000	2000	20000	Aware

Figure 8 • **Test Start**

Or use the following iCLI command to start a test.

```
# y1564 start NewReport profile MyProfile evc 1 ece 2
```

Use the following iCLI command to stop a test.

```
# y1564 start NewReport
```

Test Report

Use the following command to view the contents of a report.

```
# show y1564 report NewReport
```

Use the Save button in the GUI or the `y1564 save` command to save the report as a text file. The following is an example test report generated by the switch after running MyProfile on ECE 2 of EVC1.

```
****************************************************************************
********************************************
* Y.1564 SAM Test
****************************************************************************
********************************************
Software configuration:
  Version                    : CEServices (standalone) Version 3.63i_beta Build
1404289
  Build date                 : 2014-10-20T13:55:46+02:00
  Code revision              : e028b8fc6279
Profile configuration:
  Profile name               : MyProfile
  Description                :
  Measurement type           : Single-ended (DST loops traffic)
  DST is OAM aware           : No
  Background traffic type    : Y.1731 TST
  Delay measurement type     : Y.1731 1DM
  MEG Level                  : 7
  Dwell time                 : 500 msecs
  Frame size                 : User-defined (EMIX=u)
  User-defined frame size    : 2000 bytes
  CIR configuration test     : Enabled
  EIR configuration test     : Enabled
  Traffic policing test      : Enabled
  Service performance test: Enabled
  Acceptable FLR          : 50 permille
  Acceptable FTD          : 200 msecs
  Acceptable FDV          : 100 msecs
Report configuration:
  Report name             : NewReport
  Description             :
  Peer MAC                : 00-00-00-00-00-01
  EVC ID                  : 1
  ECE IDs - configured    : 2
  ECE IDs - actual        : 2
Configuration for ECE ID 2:
  Frame size - actual     : 2004 bytes
  UNI port - configured   : GigabitEthernet 1/1
  UNI port - actual       : GigabitEthernet 1/1
  UNI port link           : Down
  UNI port speed          : 1000 Mbps
  UNI port MTU            : 10240 bytes
  Source MAC              : 00-01-c1-00-b5-11
  Policer ID              : 3
  CIR                     : 3.00 Mbps
  CBS                     : 10000 bytes
  EIR                     : 1.00 Mbps
  EBS                     : 10000 bytes
  Policer Mode            : Color Aware
  Frame Colors            : Green and yellow
  Rate Type               : Layer 2 (data)
  VLAN Tag Type           : C-tagged only
  VLAN ID                 : 1
Overall execution status:
  Started at              : 1970-01-01T19:53:45+00:00
  Ended at                : 1970-01-01T19:56:39+00:00
  Status                  : Succeeded
************************************************ CIR configuration test
************************************************
Configuration:
  Duration per step       : 10 seconds
  Delay meas. interval    : 400 msecs
  Step count              : 5
Status:
  Started at              : 1970-01-01T19:53:45+00:00
  Ended at                : 1970-01-01T19:54:38+00:00
  Status                  : Succeeded
Step # Tx LR   Rx LR   Rx DR   Tx          Rx          Frame  Min/Avg/Max
Min/Avg/Max       Status
      (L1)    (L1)    (L2)    Frames      Frames      Loss   Delay
Delay Var.
     [Mbps]  [Mbps]  [Mbps]                      [%]    [usecs]         [usecs]
------ ------- ------- ------- ------------ ------------ ------
----------------- ----------------- ------
    1   0.59   0.59   0.59       370       370  0.00          6/7/7
0/0/0 PASS
    2   1.19   1.19   1.18       740       740  0.00          6/7/7
0/0/0 PASS
    3   1.81   1.81   1.79      1120      1120  0.00          6/7/7
0/0/0 PASS
    4   2.41   2.41   2.38      1490      1490  0.00          6/7/7
0/0/0 PASS
    5   3.02   3.02   2.99      1870      1870  0.00          6/7/7
0/0/0 PASS
```

```
************************************************ EIR configuration test
************************************************
Configuration:
  Duration                 : 10 seconds
  Delay meas. interval     : 400 msecs
Status:
  Started at               : 1970-01-01T19:54:38+00:00
  Ended at                 : 1970-01-01T19:54:48+00:00
  Status                   : Succeeded
Color  Tx LR   Rx LR   Rx DR   Tx          Rx          Frame  Min/Avg/Max
Min/Avg/Max       Status
      (L1)    (L1)    (L2)    Frames      Frames      Loss   Delay
Delay Var.
     [Mbps]  [Mbps]  [Mbps]                      [%]    [usecs]         [usecs]
------ -------- -------- -------- ------------ ------------ ------
----------------- ----------------- ------
Green    3.02   3.02   2.99      1870       1870  0.00          6/7/7
0/0/0 PASS
Yellow   0.98   0.98   0.97       619        619  0.00
N/A
************************************************ Traffic policing test
*************************************************
Configuration:
  Duration                 : 10 seconds
  Delay meas. interval     : 400 msecs
Status:
  Started at               : 1970-01-01T19:54:48+00:00
  Ended at                 : 1970-01-01T19:54:59+00:00
  Status                   : Succeeded
Color  Tx LR   Rx LR   Rx DR   Tx          Rx          Frame  Min/Avg/Max
Min/Avg/Max       Status
      (L1)    (L1)    (L2)    Frames      Frames      Loss   Delay
Delay Var.
     [Mbps]  [Mbps]  [Mbps]                      [%]    [usecs]         [usecs]
------ -------- -------- -------- ------------ ------------ ------
----------------- ----------------- ------
Green    3.01   2.91   2.88      1869       1800  3.69          6/7/7
0/0/0 PASS
Yellow   1.23   1.13   1.12       769        700  8.97
N/A
*********************************************** Service performance test
***********************************************
Configuration:
  Duration                 : 100 seconds
  Delay meas. interval     : 500 msecs
Status:
  Started at               : 1970-01-01T19:54:59+00:00
  Ended at                 : 1970-01-01T19:56:39+00:00
  Status                   : Succeeded
      Tx LR   Rx LR   Rx DR   Tx          Rx          Frame  Min/Avg/Max
Min/Avg/Max       Status
      (L1)    (L1)    (L2)    Frames      Frames      Loss   Delay
Delay Var.
     [Mbps]  [Mbps]  [Mbps]                      [%]    [usecs]         [usecs]
------ -------- -------- -------- ------------ ------------ ------
----------------- ----------------- ------
       3.02   3.02   2.99     18700      18700  0.00         6/7/36
0/0/29 PASS
**************************************************** Overall Result
****************************************************
  Ended at                 : 1970-01-01T19:56:39+00:00
  Status                   : Succeeded
```

```
***************************************************************************
*******************************************
```

Traffic Test Loop

Logical loopback with DMAC/SMAC swapping must be configured at the remote location equipment (keep in mind that round-trip measurement is actually made in that situation) because dual-ended Y.1564 test is not supported with the current software.

New traffic test loop (TT_LOOP) can be created by clicking Add New TT_LOOP and specifying the following parameters:

1. Instance: The ID of the new TT_LOOP. Once a TT_LOOP is created the configuration of that TT_LOOP can be modified by clicking the ID.
2. Name: This is a configurable name of the instance.
3. Domain: Selection between Port, EVC or VLAN domain.
4. Flow: Depending on the selection of domain. Port number if domain is “Port”, EVC ID if domain is “EVC”, VLAN ID if domain is VLAN.
5. Type: Selection between Mac_loop(All frames in the flow are looped with SMAC and DMAC swap) and OAM_loop(Loop LBM to LBR and DMM to DMR, OAM_loop is currently not supported).
6. Direction: Selection between Facility loop(Looping is done from ingress to egress) and Terminal loop (Looping is done from egress to ingress. This is currently not supported).
7. Residence Port: The port where the TT_LOOP is resident. For a EVC loop the port must be a port in the EVC. For a VLAN loop the port must be a VLAN member

When all resources are available and allocated for a given TT_LOOP instance it will be shown in the Operational state as UP, otherwise it is shown as DOWN.

Use the following command to create a MAC swapping loop on port 4 in the port domain with operational state Up.

```
(config)# traffic-test-loop 1 type mac-loop interface GigabitEthernet 1/4
direction facility domain port level 0
```

Loop domain EVC or VLAN can be used to avoid service interruptions to other services on the same physical port. Loop domain PORT is used to simplify the configuration, which eliminates dependency of EVC and VLAN settings of the switch when service interrupting is not a concern. Use mac_swap loop type when DST-OAM_AWARE is cleared in the y.1564 test profile. Use OAM loop type when DST-OAM_AWARE is set in the y.1564 test profile. The following TT_LOOP combinations are supported.

- Facility mac_swap loop in PORT domain
- Facility mac_swap loop in EVC domain
- Facilty OAM loop in EVC domain
- Terminal OAM loop in EVC domain

CHAPTER 16

SyncE Software Configuration

This document describes how to configure Synchronous Ethernet (SyncE) using the Industrial Command Line Interface (ICLI) on the device or the Web GUI. Basic knowledge of the ICLI or Web GUI configuration is a prerequisite. Similarly, knowledge about synchronization and Ethernet is required.

Synchronous Ethernet

Synchronous Ethernet (SyncE) uses a physical layer interface to pass timing from node to node in the same manner as timing is passed in SONET or SDH. SyncE, as defined by ITU-T standards such as G.8261, G.8262, G.8264, and G.781, leverages the physical layer of Ethernet to transmit frequency to remote sites. This synchronous transmission of frequency over Ethernet provides a cost-effective alternative for network designers. For SyncE to work, each network element along the synchronization path must support SyncE.

Synchronization Messaging

Network elements use Synchronization Status Messages (SSM) to inform neighboring elements about the Quality Level (QL) of the clock. SSM is used by non-Ethernet interfaces such as optical interfaces and SONET/T1/E1 SPA framers. SSM functionality provides the following key benefits.

- Prevents timing loops
- Provides fast recovery when a part of the network fails
- Ensures that a node derives timing from the most reliable clock source

To maintain a logical communication channel in synchronous network connections, Ethernet relies on a channel called the Ethernet Synchronization Messaging Channel (ESMC), based on IEEE 802.3 Organization Specific Slow Protocol standards. ESMC relays the SSM code that represents the quality level of the Ethernet Equipment Clock (EEC) in a physical layer.

The ESMC packets are received only for those ports configured as clock sources and transmitted on all SyncE interfaces in the system. These packets are then processed by the clock selection algorithm and used to select the best clock. The transmitted frame is generated based on the QL value of the selected clock source and sent to all enabled SyncE ports.

Clock Selection Algorithm

The clock selection algorithm selects the best available synchronization source from the nominated sources. The clock selection algorithm has a non-revertive behavior among clock sources with the same QL value and priority. It always selects the signal with the best QL value. The following parameters contribute to the selection process:

- Quality level
- Signal fail (QL-FAILED)
- Priority
- External commands (Manual, Auto-revertive, etc)

Configuring the Clock Source

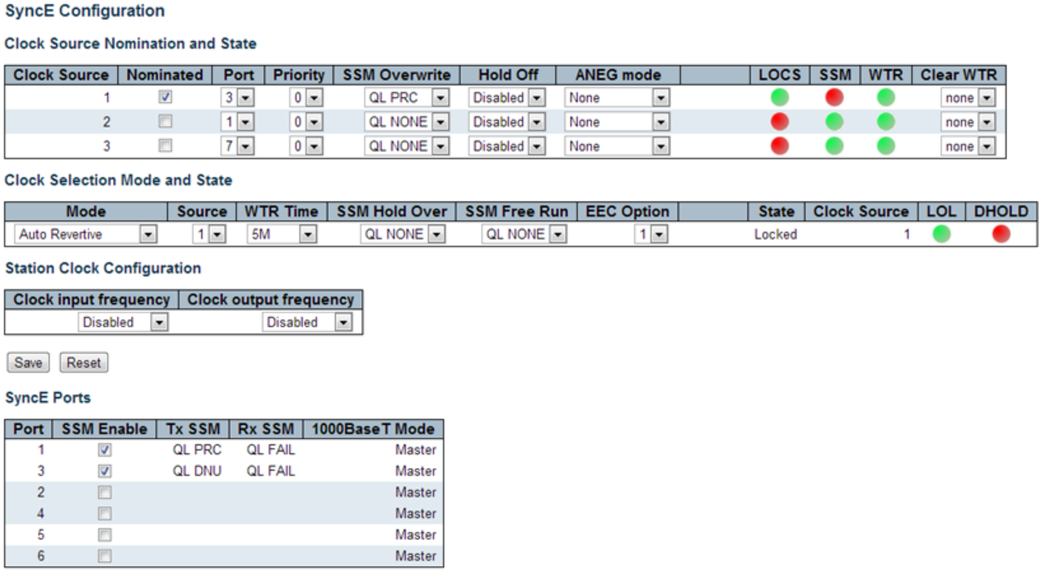
Clock Recovery

Use the following steps to configure a clock source.

1. Nominate a port to be the clock source.
2. Set the SSM overwrite if no SSM is received. Set to QL PRC.
3. If needed, enable SSM on the ports using the synchronization.

The following illustration shows the configuration settings.

Figure 1 • **Basic SyncE 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	☑	3	0	QL PRC	Disabled	None		🟢	🔴	🟢	none
2	☐	1	0	QL NONE	Disabled	None		🔴	🟢	🟢	none
3	☐	7	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		Locked	1	🟢	🔴

Station Clock Configuration

Clock input frequency	Clock output frequency
Disabled	Disabled

SyncE Ports

Port	SSM Enable	Tx SSM	Rx SSM	1000BaseT Mode
1	☑	QL PRC	QL FAIL	Master
3	☑	QL DNU	QL FAIL	Master
2	☐			Master
4	☐			Master
5	☐			Master
6	☐			Master

The state will show Locked, meaning that all Ethernet ports are transmitting with the frequency of the selected clock source, port 3 in the configuration.

The LOCS shows green when the nominated clock source is available, the SSM shows red when no SSM quality level is received, and DHOLD shows green after a while in the locked state. DHOLD is a digital hold condition for the PLL that indicates a valid holdover frequency has been calculated.

The SSM transmitted on enabled ports reflects the locked condition. On the port used as the clock source, the Tx-SSM is QL-DNU, meaning quality level - Do Not Use. This is to avoid timing loops. A receiver of the QL-DNU SSM will not use this clock as a timing source. On other ports the QL-PRC is transmitted, indicating the quality level of the clock.

The following code shows the ICLI configuration commands.

```
# conf t
(config)# network-clock clk-source 1 nominate interface GigabitEthernet
1/3
(config)# network-clock clk-source 1 ssm-overwrite prcshow version
(config)# interface GigabitEthernet 1/3
(config-if)# network-clock synchronization ssm
! Show SyncE status
# show network-clock
Selector State is: Locked to 1
Alarm State is:
Clk:        1        2        3
LOCS:    FALSE    TRUE     TRUE
SSM:     TRUE     FALSE    FALSE
WTR:     FALSE    FALSE    FALSE
LOL:     FALSE
DHOLD:   FALSE
SSM State is:
Interface                    Tx SSM      Rx SSM Mode
GigabitEthernet 1/1          QL_PRC      QL_FAIL Master
GigabitEthernet 1/3          QL_DNU      QL_FAIL Master
```

Clock Redundancy

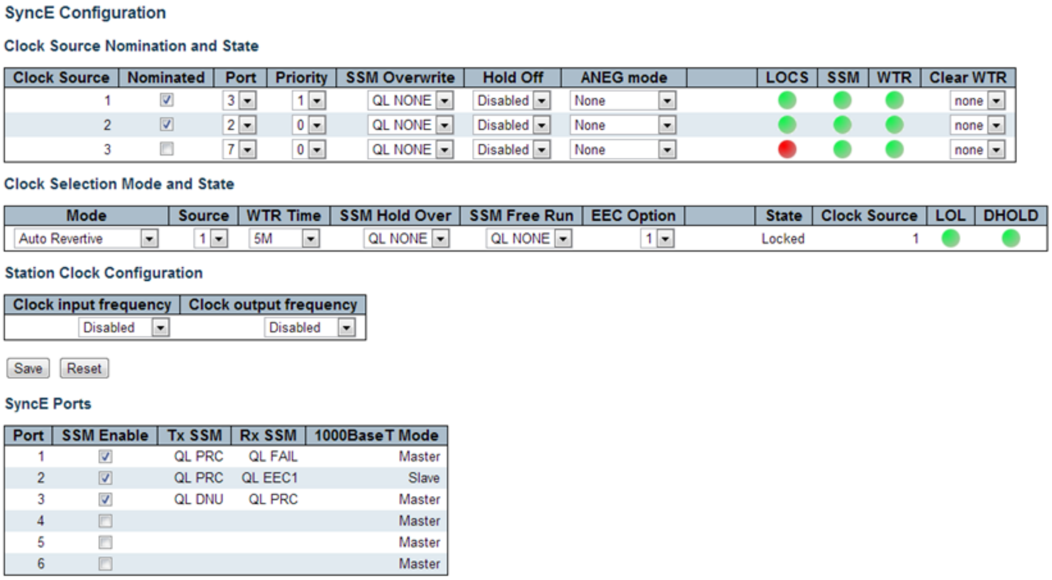
It is possible to configure up to three clock sources. Two sources from any of the Ethernet ports and the third from an external clock input. Based on the priority and QL of these clock sources, the best source is selected. Use the following steps to configure the clock.

1. Nominate the clock source
2. Set the priority
3. Enable SSM on the ports using the synchronization.

Note: QL overrides the priority. If port 3 receives QL-PRC and port 2 receives only QL-EEC1, but port 2 has higher priority (lowest number, 0), port 3 is selected.

The following illustration shows the configuration settings.

Figure 2 • **Clock Redundancy**



SyncE Configuration

Clock Source Nomination and State

Clock Source	Nominated	Port	Priority	SSM Overwrite	Hold Off	ANEG mode		LOCS	SSM	WTR	Clear WTR
1	☑	3	1	QL NONE	Disabled	None		🟢	🟢	🟢	none
2	☑	2	0	QL NONE	Disabled	None		🟢	🟢	🟢	none
3	□	7	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		Locked	1	🟢	🟢

Station Clock Configuration

Clock input frequency	Clock output frequency
Disabled	Disabled

SyncE Ports

Port	SSM Enable	Tx SSM	Rx SSM	1000BaseT Mode
1	☑	QL PRC	QL FAIL	Master
2	☑	QL PRC	QL EEC1	Slave
3	☑	QL DNU	QL PRC	Master
4	□			Master
5	□			Master
6	□			Master

The following code shows the ICLI configuration commands.

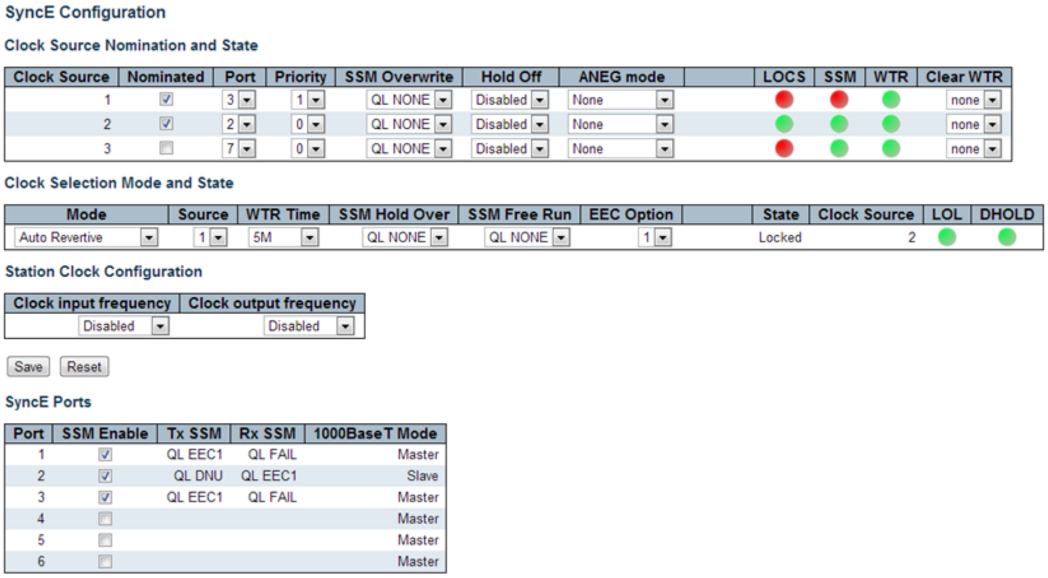
```
# conf t
(config)# network-clock clk-source 1 nominate interface GigabitEthernet
1/3
(config)# network-clock clk-source 2 nominate interface GigabitEthernet
1/2
(config)# network-clock clk-source 1 priority 0
(config)# interface GigabitEthernet 1/1-3
(config-if)# network-clock synchronization ssm
```

Clock Redundancy with Input Fail

If the selected source fails, the other source is selected because the default mode setting is Auto-revertive.

The following illustration shows the configuration settings.

Figure 3 • **Selected Clock Source Failure**



SyncE Configuration

Clock Source Nomination and State

Clock Source	Nominated	Port	Priority	SSM Overwrite	Hold Off	ANEG mode		LOCS	SSM	WTR	Clear WTR
1	☑	3	1	QL NONE	Disabled	None		🔴	🔴	🟢	none
2	☑	2	0	QL NONE	Disabled	None		🟢	🟢	🟢	none
3	☐	7	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		Locked	2	🟢	🟢

Station Clock Configuration

Clock input frequency	Clock output frequency
Disabled	Disabled

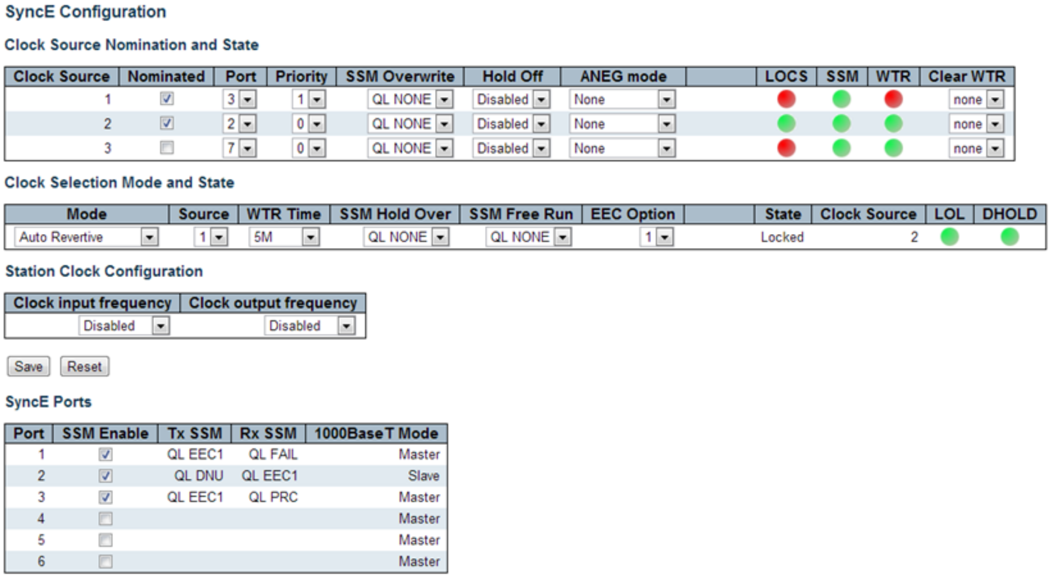
Save Reset

SyncE Ports

Port	SSM Enable	Tx SSM	Rx SSM	1000BaseT Mode
1	☑	QL EEC1	QL FAIL	Master
2	☑	QL DNU	QL EEC1	Slave
3	☑	QL EEC1	QL FAIL	Master
4	☐			Master
5	☐			Master
6	☐			Master

When port 3 is restored, the wait to restore (WTR) timer is started. When the WTR timer expires, the primary port is again selected as the clock source as follows:

Figure 4 • **Active Wait to Restore Timer**



SyncE Configuration

Clock Source Nomination and State

Clock Source	Nominated	Port	Priority	SSM Overwrite	Hold Off	ANEG mode		LOCS	SSM	WTR	Clear WTR
1	☑	3	1	QL NONE	Disabled	None		🔴	🟢	🔴	none
2	☑	2	0	QL NONE	Disabled	None		🟢	🟢	🟢	none
3	☐	7	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		Locked	2	🟢	🟢

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	☑	QL EEC1	QL FAIL	Master
2	☑	QL DNU	QL EEC1	Slave
3	☑	QL EEC1	QL PRC	Master
4	☐			Master
5	☐			Master
6	☐			Master

Clock Selection Modes

The definition of the best clock source is the one with the highest QL and the highest priority among the ones with equal QL.

The available clock selection modes are as follows.

Manual - No clock selection occurs as the clock source is strictly what is stated in the Source field. 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 port selected clock source will become the source.

Auto NonRevertive - Clock selection of the best clock source is only done when the selected clock fails.

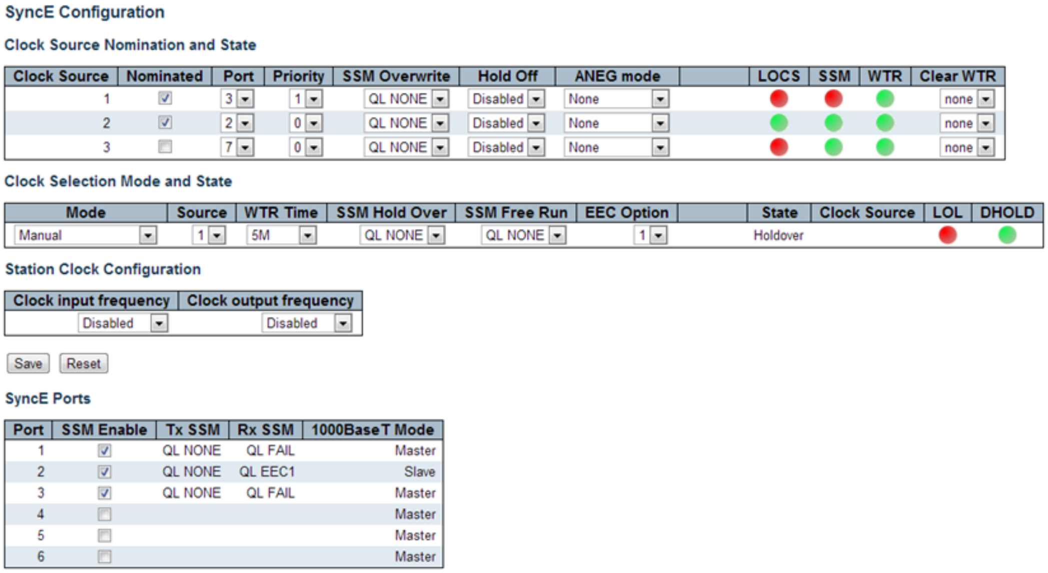
Auto Revertive - Clock selection of the best clock source is constantly done. This is the default setting.

Force Hold Over - Clock selector is forced to hold over state.

Force Free Run - Clock selector is forced to free run state.

The following illustration shows the configuration settings.

Figure 5 • **Selected Source Failure in Manual Mode with no Switch Over**



SyncE Configuration

Clock Source Nomination and State

Clock Source	Nominated	Port	Priority	SSM Overwrite	Hold Off	ANEG mode		LOCS	SSM	WTR	Clear WTR
1	☑	3	1	QL NONE	Disabled	None		🔴	🔴	🟢	none
2	☑	2	0	QL NONE	Disabled	None		🟢	🟢	🟢	none
3	□	7	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
Manual	1	5M	QL NONE	QL NONE	1		Holdover		🔴	🟢

Station Clock Configuration

Clock input frequency	Clock output frequency
Disabled	Disabled

SyncE Ports

Port	SSM Enable	Tx SSM	Rx SSM	1000BaseT Mode
1	☑	QL NONE	QL FAIL	Master
2	☑	QL NONE	QL EEC1	Slave
3	☑	QL NONE	QL FAIL	Master
4	□			Master
5	□			Master
6	□			Master

Manual mode is used to force the selection of a specific source. This may be used to switch back to a primary source if auto-nonrevertive mode is selected and the failure is cleared.

Manual To Selected mode is used to freeze the current clock source in case of a failure upon switchover.

The following code shows the ICLI configuration command for the clock selection mode.

```
# conf t
(config)# network-clock selector manual clk-source 0
```

WTR and Hold Off Timers

Two timers are available:

- WTR (Wait to restore) Timer
- Hold Off Timer

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 the WTR timer is cleared.

The Hold Off timer delays the active loss of clock by an amount of time. The clock selector will not change clock source if the loss of clock condition is cleared within this time.

The following ICLI timer configuration commands configure a WTR of 1 minute and a hold-off on clock source 1 to 300 ms.

```
# conf t
(config)# network-clock wait-to-restore  1
(config)# network-clock clk-source 1 hold-timeout 3
```

ANEG Mode

Auto negotiation (ANEG) mode is relevant for 1000BaseT ports only. To recover the clock from a port, it must be negotiated to Slave mode. To distribute the clock, the port must be negotiated to Master mode. The following 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.

Forced Slave - The port will be forced to master mode. The selected port in locked state will always be negotiated to slave if possible.

The following code shows the related ICLI command.

```
# conf t
(config)# network-clock clk-source 1 aneg-mode slave
```

Station Clock

It is possible to select an input clock signal and to generate an output clock signal. Both signals can be 1.544 MHz, 2.048 MHz, or 10 MHz individually selected.

The input clock signal can be used as the clock source and is nominated as clock source 3

The "port" number is the last Ethernet port plus 1 or S-CLK (clk-in) dependent on release.

Because this input clock signal carries no SSM, an SSM overwrite quality level must be set, as follows.

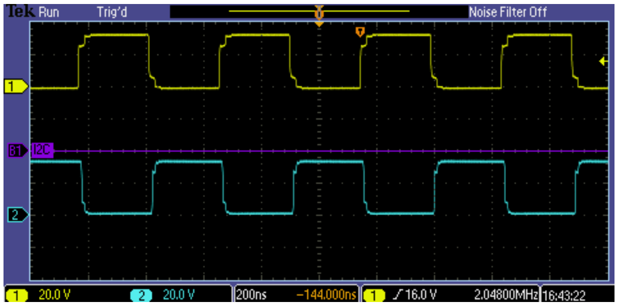
```
# conf t
(config)# network-clock input-source 10mhz
(config)# network-clock output-source 2048khz
(config)# network-clock clk-source 3 nominate clk-in
(config)# network-clock clk-source 3 ssm-overwrite eec1
```

The following illustration shows the output frequency measured.

- Channel 1 is remote node used as source
- Channel 2 is the local node that is locked to remote node

Note: SyncE provides frequency synchronization, not phase, so the phase between the two nodes are arbitrary.

Figure 6 • **Output Frequency Measured**



PTP as Clock Source

From release 3.65, it is possible to use a PTP instance as clock source.

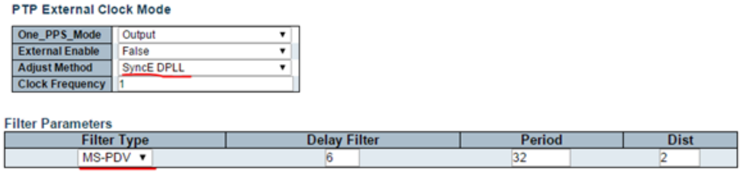
Pre-requisites

Ensure that the following parameters are set as shown in the following illustration.

Adjustment Method = SyncE DPLL

Filter Type = MS-PDV

Figure 7 • **PTP External Clock Mode**



PTP External Clock Mode

One_PPS_Mode	Output
External Enable	False
Adjust Method	SyncE DPLL
Clock Frequency	1

Filter Parameters

Filter Type	Delay Filter	Period	Dist
MS-PDV	6	32	2

Configuring PTP as Clock Source using WebGUI

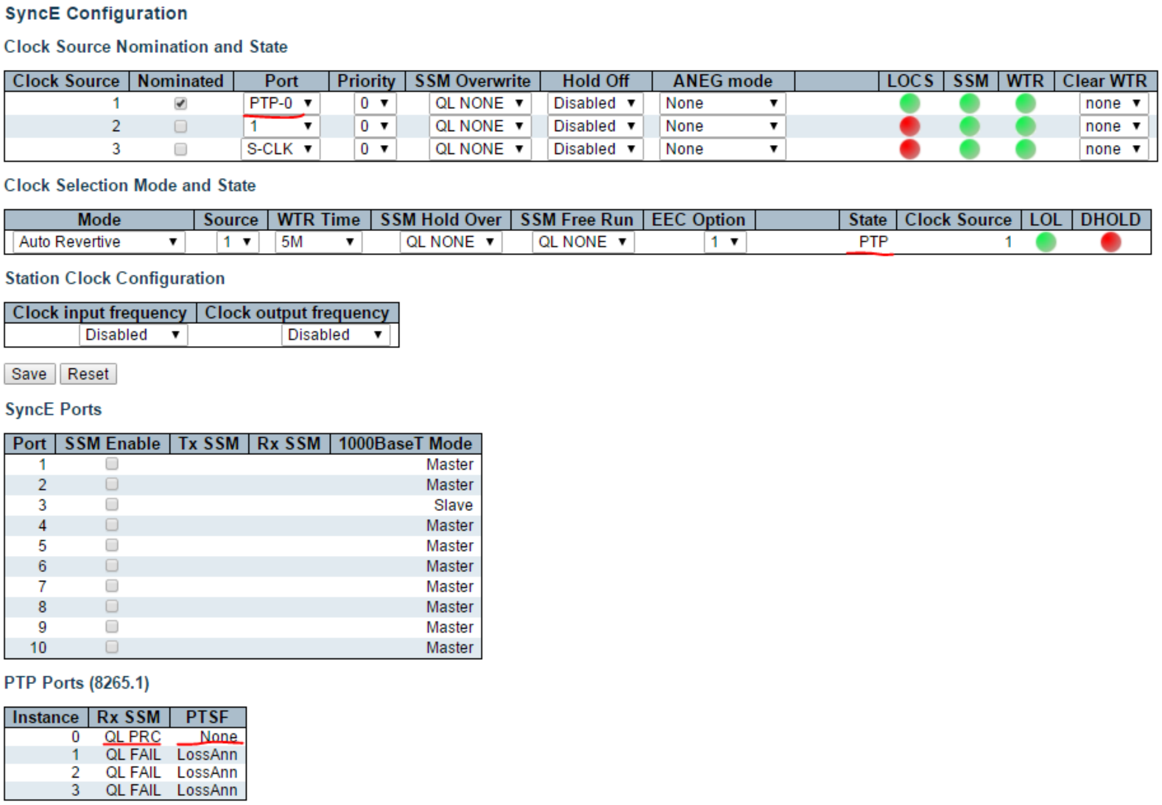
To configure PTP as a clock source, you need to perform the following step.

1. Go to **SyncE Configuration** page and configure as shown in the following illustration.

Note The status of the PTP instance is shown in the PTP Ports (G.8265.1)

- RX SSM shows the quality level of the PTP clock class converted to SyncE QL. F.ex. PTP Clock class 84 = QL PRC
- PTSF (Packet Timing Signal Fail)
  - None means no error
  - Unusable means no valid PTP source

Figure 8 • SyncE Configuration



SyncE Configuration

Clock Source Nomination and State

Clock Source	Nominated	Port	Priority	SSM Overwrite	Hold Off	ANEG mode		LOCS	SSM	WTR	Clear WTR
1	☑	PTP-0 ▼	0 ▼	QL NONE ▼	Disabled ▼	None ▼		🟢	🟢	🟢	none ▼
2	☐	1 ▼	0 ▼	QL NONE ▼	Disabled ▼	None ▼		🔴	🟢	🟢	none ▼
3	☐	S-CLK ▼	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 ▼		PTP	1	🟢	🔴

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	☐			Master
3	☐			Slave
4	☐			Master
5	☐			Master
6	☐			Master
7	☐			Master
8	☐			Master
9	☐			Master
10	☐			Master

PTP Ports (8265.1)

Instance	Rx SSM	PTSF
0	QL PRC	None
1	QL FAIL	LossAnn
2	QL FAIL	LossAnn
3	QL FAIL	LossAnn

Configuring Clock Class on Master Node using CLI

Execute the following command to set Clock Class on master node.

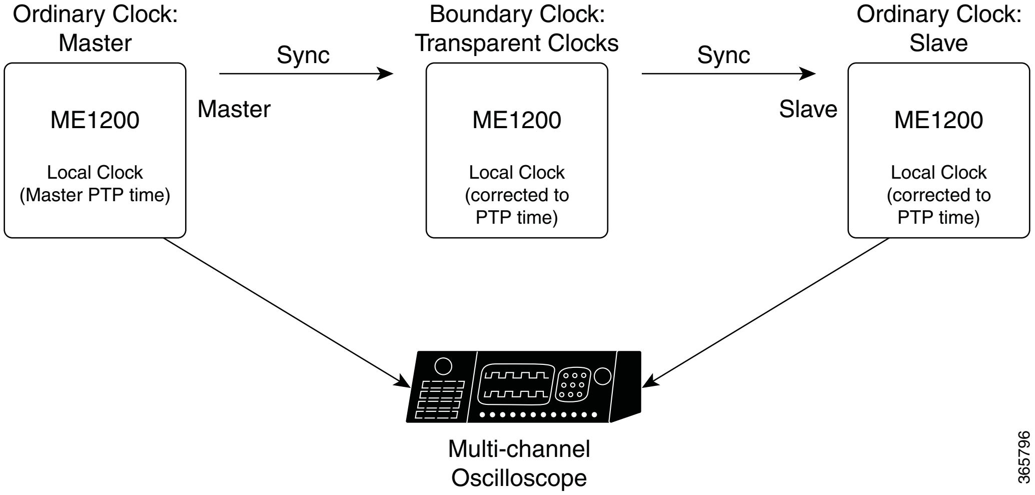
```
(config)# debug ptp 0 class 84
```

IEEE1588 and NTP Configuration

This document describes how to configure the IEEE1588v2 Precision Time Protocol (PTP) in Cisco ME1200. The Network Time Protocol (NTP) configuration is also described, including how to combine NTP and IEEE1588v2.

The following illustration shows a simple network configuration based on three connected nodes. The physical connections between the nodes are 1 Gbps copper or optical (SFP).

Figure 1 • **Network Configuration**



Configuration with Profile

IEEE1588 PTP implementation follows the IEEE1588-2008 (v2) standard. The standard allows other standardization bodies to create profiles and those use a specific set of parameters, optimizing the use of time synchronization for a specific purpose. The profiles are also allowed to add new additional features and replace the default Best Master Selection Algorithm (BMCA) with a profile-specific BMCA.

The ME1200 supports:

- Standard IEEE1588 profile
- ITU-T G.8265.1 Profile for frequency synchronization in a PTP-unaware network (from release 3.65)

- ITU-T G.8275.1 Profile for frequency and phase synchronization in a fully PTP-aware network (from release 3.66)
- No Profile

When creating a new PTP instance, it is possible to specify one of the above profiles, and all parameters are set according to the profile. If the profile requires the use of a BMCA other than the default BMCA, then this BMCA is used.

Note: It is possible to change parameters after a profile has been selected, but doing so might violate the profile.

The following sections demonstrate G.8265.1 profile and G.8275.1 profile configurations.

Profile ITU-T G.8265.1

This profile uses the unicast Ipv4 protocol, therefore the slaves must be configured with the corresponding master(s). This profile is also designed for PTP-unaware networks, therefore the advanced MS-PDV filter algorithm is used.

In this example, the nodes use VLAN 1 for PTP communications. For the IP unicast profile G.8265.1, the nodes have IP addresses of 192.0.2.1-2/24.

It is also assumed that the PTP master is frequency locked to a primary reference clock (PRC).

Configuring Slave and Master using CLI

To configure a slave and a master, execute the following commands.

```
!Master
ptp 0 mode master onestep ip4uni oneway profile g8265.1 mep 1
ptp ext output ltc-frequency
interface GigabitEthernet 1/3
ptp 0

!Slave G.8265.1 Profile
network-clock clk-source 1 nominate ptp 0
ptp ms-pdv  min-phase 20 apr 1
ptp 0 mode slave onestep ip4uni oneway id 00:01:c1:ff:fe:00:b3:b0 vid 1 0 profile g8265.1
mep 1
ptp 0 priority1 255
ptp 0 filter delay 6 filter-type ms-pdv period 32 dist 2
ptp 0 uni 0 duration 100 192.0.2.1
ptp ext output synce-dpll
!
interface GigabitEthernet 1/3
 ptp 0
```

Verifying Configuration using CLI

To verify the proper configuration for Port-Timer and Phy-timestamper for copper ports, execute the following CLI commands.

```
show ptp 0 port-state
Port  Enabled  PTP-State  Internal  Link  Port-Timer  Vlan-forw  Phy-timestamper
Peer-delay
----  -------  ---------  --------  ----  ----------  ---------  ---------------
----------
   1  FALSE    dsbl       FALSE     Down  In Sync     Discard    FALSE            OK
   2  FALSE    dsbl       FALSE     Down  In Sync     Discard    FALSE            OK
   3  TRUE     slve       FALSE     Up    In Sync     Forward    TRUE             OK
```

Note If 1588 PHY is used, then Phy-timestamper = True, and Port-Timer = In-sync

Troubleshooting

Ensure that the PTP-State on the ports are as expected.

If the port-timer shows out-of-sync, then the PHY is not synchronized to the switch. The cause for this might be that the One_pps_mode is NOT set to Output.

If Vlan-forw shows Discard, then VLAN configured for PTP does not match VLAN port setting.

SyncE Configuration

TU-T.8275.1 also uses SyncE as a frequency source.

Configuring SyncE using CLI

To configure SyncE, execute the following commands.

```
!Master
network-clock ssm-freerun eec1
network-clock selector freerun
ptp 0 mode master onestep ethernet twoway vid 1 0 profile g8275.1
ptp 0 priority2 60
ptp ext output synce-dpll
interface GigabitEthernet 1/3
 switchport mode hybrid
 network-clock synchronization ssm
 ptp 0

!Boundary Clock
network-clock clk-source 1 nominate interface GigabitEthernet 1/3
ptp 0 mode boundary onestep ethernet twoway vid 1 0 profile g8275.1
ptp ext output ltc-phase
interface GigabitEthernet 1/3
 switchport mode hybrid
 network-clock synchronization ssm
 ptp 0
 !
interface GigabitEthernet 1/4
 switchport mode hybrid
 media-type rj45
 network-clock synchronization ssm
 ptp 0

! Slave
network-clock clk-source 1 nominate interface GigabitEthernet 1/4
ptp 0 mode slave onestep ethernet twoway vid 1 0 profile g8275.1
ptp ext output ltc-phase
interface GigabitEthernet 1/4
 switchport mode hybrid
 network-clock synchronization ssm
 ptp 0
```

Verifying Configuration using CLI

To verify the proper configuration for Port-Timer and Phy-timestamper for copper ports, execute the following CLI commands.

```
show ptp 0 port-state
Port  Enabled  PTP-State  Internal  Link  Port-Timer  Vlan-forw  Phy-timestamper
Peer-delay
----  -------  ---------  --------  ----  ----------  ---------  ---------------
----------
   1  FALSE    dsbl       FALSE     Down  In Sync     Discard    FALSE            OK
   2  FALSE    dsbl       FALSE     Down  In Sync     Discard    FALSE            OK
   3  TRUE     slve       FALSE     Up    In Sync     Forward    TRUE             OK
```

Note If 1588 PHY is used, then Phy-timestamper = True and Port-Timer = In-sync

Troubleshooting

Ensure that the PTP-State on the ports are as expected.

If the port-timer shows out-of-sync, then the PHY is not synchronized to the switch. The cause for this could be that the One_pps_mode is NOT set to Output.

If Vlan-forw shows Discard, then the VLAN configured for PTP does not match the VLAN port setting.

Other Parameters for G.8275.1 Profile

The following commands set the other parameters defined in the G.8275.1 standard

```
(config)# ptp ho-spec cat1 <0-x> cat2 <0-x> cat3 <0-x>
(config)# ptp 0 localpriority <1-255>
(config-if)# ptp 0 localpriority <1-255>
(config-if)# ptp 0 mcast-dest  <default | link-local>
(config-if)# ptp 0 not_slave
```

where,

- ho-spec - Holdover specification for G8275 PTP clocks
- localpriority - Local priority for G8275.1 BMC algorithm (1 is highest priority)
- localpriority - Local priority pr port for G8275.1 BMC algorithm (1 is highest priority)
- mcast-dest - Multicast destination address type for the port
- not-slave - “Not-slave' attribute for G8275.1 BMC algorithm

Note Priority1 is not used in G.8275.1. Instead, the local priority is used. The priority order is Priority2 and then Local priority.

Configuration Without Profile

For applications other than 1588, G.8265.1 and G.8275.1, use No Profile and select the parameters to match the application.

Configuring Master through E2E-Transparent Clock to Slave on Layer 2 (No Profile)

Configuring Master Through Transparent Clock to Slave on Layer 2 using CLI

To configure master through transparent clock to slave on layer 2, execute the following commands.

```
!Master
ptp 0 mode boundary onestep ethernet twoway vid 1 0 mep 1
ptp 0 priority1 50
ptp ext output ltc-freq
interface GigabitEthernet 1/3
 switchport mode hybrid
 ptp 0

!Transparent Clock
ptp 0 mode e2etransparent onestep ethernet twoway vid 1 0 mep 1
ptp ext output ltc-freq
interface GigabitEthernet 1/3
 switchport mode hybrid
 ptp 0
 !
interface GigabitEthernet 1/4
 switchport mode hybrid
 ptp 0

! Slave
ptp 0 mode boundary onestep ethernet twoway vid 1 0 mep 1
ptp ext output ltc-freq
interface GigabitEthernet 1/4
 switchport mode hybrid
 ptp 0
```

.Verifying Configuration using CLI

To verify the proper configuration for Port-Timer and Phy-timestamper for copper ports, execute the following CLI commands.

```
show ptp 0 port-state
# sh ptp 0 port-st
Port  Enabled  PTP-State  Internal  Link  Port-Timer  Vlan-forw  Phy-timestamper
Peer-delay
----  -------  ---------  --------  ----  ----------  ---------  ---------------
----------
   1  FALSE    dsbl       FALSE     Down  In Sync     Discard    FALSE           OK
   2  FALSE    dsbl       FALSE     Down  In Sync     Discard    FALSE           OK
   3  TRUE     e2et       FALSE     Up    In Sync     Forward    TRUE            OK
   4  TRUE     e2et       FALSE     Up    In Sync     Forward    TRUE            OK
```

Troubleshooting

Ensure that the PTP-State on the ports are as expected.

If the port-timer shows the PTP-State is out-of-sync, then the PHY is not synchronized to the switch. The reason for this could be that the One_pps_mode is not set to Output.

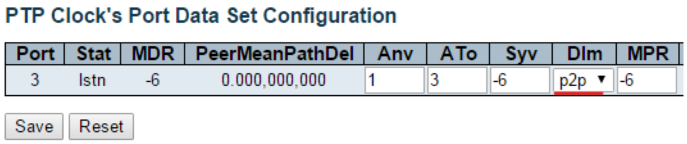
If Vlan-forw shows Discard, then VLAN configured for PTP does not match the VLAN port setting.

Configuring Master through P2P-Transparent Clock to Slave on Layer 2 (No Profile)

This configuration is very similar to the E2E configuration discussed in Configuring Master through E2E-Transparent Clock to Slave on Layer 2 (No Profile), with the following changes.

- Master and Slave nodes (Boundary Clock) - Set Dlm (Delay measurement) to p2p.

Figure 2 • **Port Data Set Configuration**

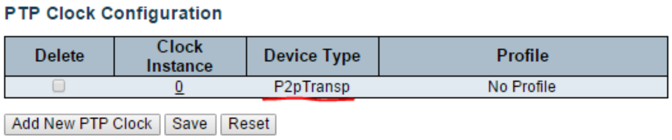


PTP Clock's Port Data Set Configuration

Port	Stat	MDR	PeerMeanPathDel	Anv	ATo	Syv	Dlm	MPR
3	lstn	-6	0.000,000,000	1	3	-6	p2p ▾	-6

- Set Dlm (Delay measurement) to p2p - Create the PTP instance as P2pTransp.

Figure 3 • **PTP Clock Configuration**



PTP Clock Configuration

Delete	Clock Instance	Device Type	Profile
□	0	P2pTransp	No Profile

Other Parameters

There are two types of PTP parameters:

- IEEE1588 standard parameters
- Filter parameters

The naming and value types follow the IEEE1588 standard, so consult the standard for further description.

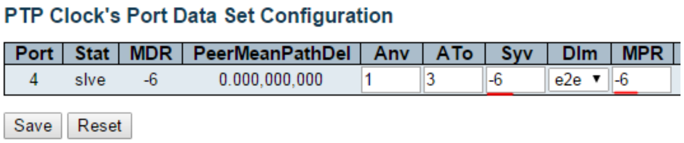
For description of filter parameters, click the web help on the application interface. The parameters can be adjusted through the PTP instance.

Managing Sync and Delay Request rates

The default sync rate is 1 f/s and the default delay-request rate is 1 f/8 s. Increasing these rates will improve accuracy. To adjust the rates

Click the PTP instance and then for rates of 64 f/s, configure as shown in the following illustration.

Figure 17-1 ***Manage Parameters***



PTP Clock's Port Data Set Configuration

Port	Stat	MDR	PeerMeanPathDel	Anv	ATo	Syv	Dlm	MPR
4	slve	-6	0.000,000,000	1	3	-6	e2e ▾	-6

NTP and Time Zone Configuration

The Network Time Protocol (NTP) synchronizes the time of day among a set of distributed time servers and clients. This helps a user correlate events from system logs and other time-specific events from multiple network devices. NTP uses the User Datagram Protocol (UDP) as its transport protocol. All NTP communications use Coordinated Universal Time (UTC).

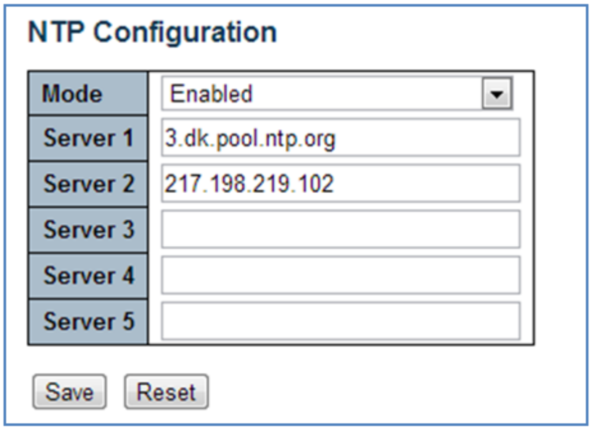
NTP version 4 is implemented, although it is disabled by default. The NTP IPv4 or IPv6 address can be configured and a maximum of five servers is supported.

Configuring NTP using WebGUI

To configure the NTP and server address

- Go to **Configuration** > **System** > **NTP**, and set the configuration details as shown in the following illustration.

Figure 17-2 NTP Configuration



NTP Configuration

Mode	Enabled
Server 1	3.dk.pool.ntp.org
Server 2	217.198.219.102
Server 3	
Server 4	
Server 5	

Configuring NTP using CLI

To configure the NTP and server address, execute the following CLI commands.

```
# configure terminal
! Enable Enable NTP and set server address
(config)# ntp
(config)# ntp server 1 ip-address 3.dk.pool.ntp.org
(config)# ntp server 1 ip-address 217.198.219.102
```

The software allows the user to configure the local time zone. The switch must be configured to acquire the time from an NTP server. The default time zone is configured as None.

An acronym may optionally be assigned to a selected time zone. The acronym can be up to 16 alpha-numeric characters in length, allowing special characters such as, '-' (hyphen), '.' (period), and '_' (underscore). The acronym is case sensitive.

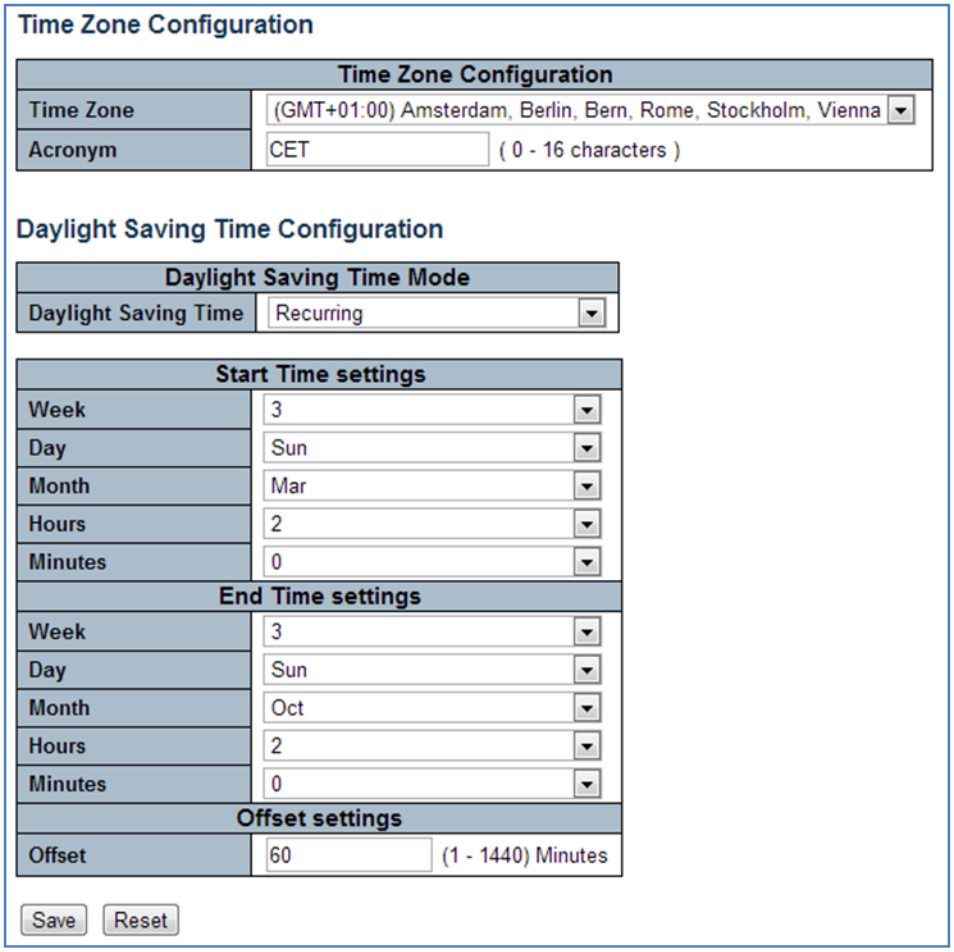
The software will allow the user to configure Daylight Savings Time (DST) if and when it occurs for a time zone. When configured, the system time will automatically adjust during Daylight Savings Time.

Configuring Time Zone using Web GUI

To configure the Time Zone

- Go to **Configuration** > **System** > **Time**, and set the configuration details as shown in the following illustration.

Figure 17-3 Time Zone Configuration



Time Zone Configuration

Time Zone Configuration	
Time Zone	(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Acronym	CET (0 - 16 characters)

Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Recurring

Start Time settings	
Week	3
Day	Sun
Month	Mar
Hours	2
Minutes	0
End Time settings	
Week	3
Day	Sun
Month	Oct
Hours	2
Minutes	0
Offset settings	
Offset	60 (1 - 1440) Minutes

Configuring Time Zone using CLI

To configure the Time Zone, execute the following CLI commands.

```
# configure terminal
! Set time zone and Daylight saving
(config)# clock summer-time CET recurring 3 7 3 02:00 3 7 10 02:00 60 (config)# clock
timezone CET 1
```

PTP and System Clock (NTP) Synchronization

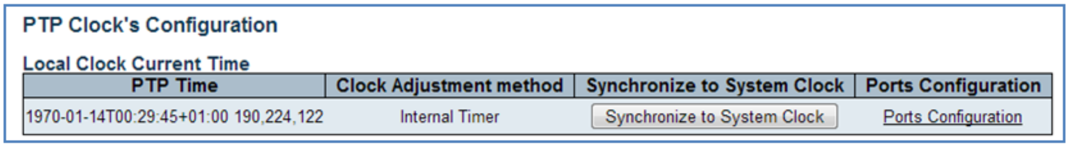
Normally, the PTP clock comes from an IEEE1588 Grand Master, but if a Grand Master is not available, it is possible to use the NTP time as a PTP clock.

Synchronizing PTP and System Clock (NTP) using Web GUI

To configure PTP and NTP

- Go to **Configuration** > **PTP** > **Clock**, and click **Synchronize to System Clock** to use the local system clock as the PTP clock.

Figure 17-4 PTP Clock Synchronization



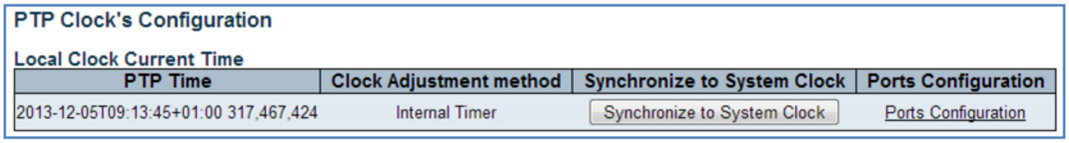
PTP Clock's Configuration

Local Clock Current Time

PTP Time	Clock Adjustment method	Synchronize to System Clock	Ports Configuration
1970-01-14T00:29:45+01:00 190,224,122	Internal Timer	Synchronize to System Clock	Ports Configuration

The page gets updated.

Figure 17-5 PTP Clock Update



PTP Clock's Configuration

Local Clock Current Time

PTP Time	Clock Adjustment method	Synchronize to System Clock	Ports Configuration
2013-12-05T09:13:45+01:00 317,467,424	Internal Timer	Synchronize to System Clock	Ports Configuration

Synchronizing PTP and System Clock (NTP) using CLI

To configure PTP and NTP, execute the following CLI commands.

```
# configure terminal
! Synchronize PTP time to System Clock
# ptp 0 local-clock update
```

It is also possible to continuously (each second) synchronize the PTP time and System time. This is done using the following CLI commands.

```
# configure terminal
! Synchronize PTP time to System Clock
(config)# ptp system-time set
! Or Synchronize System Clock to PTP time
(config)# ptp system-time get
```

CHAPTER 18

Configure the DHCP Client

This document describes basic usage of Industrial Command Line Interface (ICLI) to configure the DHCP client with a Cisco ME1200.

The ICLI is a comprehensive management interface on the device. It is the only management interface accessible on the serial console. Even if there is no network connectivity, the device can still be managed using a serial connection. The following commands assume that the device is powered on and the serial port has a functional connection to a computer console. Serial port setting should be as follows:

- 115200 baud
- No parity
- 8 data bits
- 1 stop bit
- No flow control

The computer must be running a terminal emulator such as TeraTerm or PuTTY on Windows, or Minicom on Linux.

The '#' denotes the user prompt.

```
# configure terminal
(config)# hostname Switch
Switch(config)# end
```

DHCP Client

When enabled, the DHCP client within the switch application software sends out requests for IP address configuration. When the requests are received by a DHCP server on the network the server searches through its pool of available IP addresses, allocates one, and returns it to the DHCP client. The returned information typically includes IP address, netmask, and default gateway, but may also contain other information such as Domain Name Service (DNS) server addresses.

Note: IP addresses can only be assigned to VLAN interfaces.

The interface configuration mode is used to configure the parameters for an interface or a range of interfaces. An interface can be a physical port, VLAN, or other virtual interface. The interface configuration mode is distinguished further according to the type of interface. The command prompt for each type of interface is slightly different.

The VLAN interface configuration mode is used to configure the parameters of a VLAN interface. The following sections describe the commands to access the VLAN interface configuration mode

Static IP Address

In the application software, VLAN 1 is typically used as the management VLAN. The objective is to assign an IP address to the device on VLAN 1. The following static setup is also the default setup.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if-vlan)# ip address 192.0.2.1 255.255.255.0
Switch(config-if-vlan)# end
```

DHCP Address

The application software includes a DHCP client, which must be enabled to automatically obtain an IP address from a DHCP server located on the network.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if-vlan)# ip address dhcp
Switch(config-if-vlan)# end
```

DHCP Address with Fallback

It is a good practice to default to an iP address after a timeout period for those instances where there is no DHCP server on the network.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if-vlan)# ip address dhcp fallback 192.0.2.1 255.255.255.0
Switch(config-if-vlan)# end
```

Display IP Address

The following output is displayed after the static address has been set up.

```
Switch# show ip interface brief
Interface Address              Method   Status
--------- -------------------- -------- ------
VLAN 1     192.0.2.2/24         Manual   UP
Switch#
```

Although the output says "Interface 200000001", this is equal to VLAN interface 1. The interface index range 200000000-299999999 is used for VLAN interfaces.

When the DHCP negotiation is successful the following response is displayed.

```
Switch# show ip interface brief
Interface Address              Method   Status
--------- -------------------- -------- ------
VLAN 1     10.10.132.82/23      DHCP     UP
Switch#
```

The command `show ip interface brief` displays configured and active IP interfaces. Active interfaces should show a status of UP. If this status is not seen, there may be no link on any port. The fallback IP of 192.0.2.1 is assigned if the DHCP negotiation fails. The following command displays DHCP session statistics.

```
Switch# show ip dhcp detailed statistics client
GigabitEthernet 1/1 Statistics:
-------------------------------
Rx Discover:                   0   Tx Discover:                   4
Rx Offer:                      1   Tx Offer:                      0
Rx Request:                     0   Tx Request:                     17
Rx Decline:                     0   Tx Decline:                      0
Rx ACK:                        17   Tx ACK:                          0
Rx NAK:                         0   Tx NAK:                          0
Rx Release:                     0   Tx Release:                      0
Rx Inform:                      0   Tx Inform:                       0
Rx Lease Query:                 0   Tx Lease Query:                  0
Rx Lease Unassigned:            0   Tx Lease Unassigned:             0
Rx Lease Unknown:               0   Tx Lease Unknown:                0
Rx Lease Active:                0   Tx Lease Active:                 0
Rx Lease Active:                0   Tx Lease Active:                 0
Rx Discarded checksum error:    0
Switch#
```

Another way to show the IP address is by displaying the actual VLAN.

```
Switch# show interface vlan 1
VLAN1
  LINK: 00-01-c1-00-b1-10 Mtu:1500 <UP BROADCAST RUNNING MULTICAST>
  IPv4: 10.10.132.82/23 10.10.133.255
  DHCP: State: BOUND server: 10.10.132.2
  IPv6: fe80:2::201:c1ff:fe00:b110/64 <ANYCAST TENTATIVE AUTOCONF>
Switch#
```

Using the Obtained Network Connection

Once the basic system configuration is complete, management connectivity can be verified by issuing a `ping` command to a known external IP address.

```
Switch# ping ip 10.10.130.66
PING server 10.10.130.66, 56 bytes of data.
64 bytes from 10.10.130.66: icmp_seq=0, time=10ms
64 bytes from 10.10.130.66: icmp_seq=1, time=10ms
64 bytes from 10.10.130.66: icmp_seq=2, time=0ms
64 bytes from 10.10.130.66: icmp_seq=3, time=0ms
64 bytes from 10.10.130.66: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
Switch#
```

If the ping is successful, network logins can now be performed using **telnet** or **ssh** to the address on VLAN interface 1.

Saving the Configuration to FLASH

The current configuration of the device does not survive across reboots. Use the following commands to save running-config to FLASH storage under the name startup-config.

```
Switch# copy running-config startup-config
Building configuration...
% Saving 1223 bytes to flash:startup-config
Switch#
```

The startup-config file is read and executed on every boot. It is also used to restore the running configuration of the system to the last saved state.

Getting an IP Address

Obtaining an IP address is not successful when two switches have the same MAC address. A MAC address must be unique because the DHCP server binds the MAC address and the IP address. Use the following steps to specify a unique MAC address to get an IP address from the network.

```
Switch# platform debug allow
Switch# debug board
Board MAC Address: 00-01-c1-00-b1-10
Board ID         : 34
Board Type Active: Sandino
Switch# debug board mac 00-01-c1-00-b1-20
Switch#
```

CHAPTER 19

IP Multicast Configuration

This document provides steps for deploying the IPMC profile, IGMP/MLD snooping and proxy, and MVR to manage IPMC traffic forwarding using ICLI commands and the Web GUI. It requires familiarity with IP/HTTP technology and experience in setting up an OS application service.

A network equipment device running Cisco ME1200software is managed on a platform that may be a computer running an IP-capable OS (for example, FreeBSD®, Linux® or WINDOWS®).

- To use ICLI as the management interface, requires a serial console connection between the device and the management platform. No network connection is required to use ICLI, but the terminal emulator software has to be installed.
- To use the Web GUI as the management interface, requires an active network connection for the management platform to access the device using a Web browser and IP communication.

IGMP/MLD Snooping

IP multicast reduces the IP broadcasting data traffic efforts by forwarding the data frames to only those network equipments that expect the designated frames proposing group registration. It is commonly deployed for triple play services (data, voice, and video) such as network conference system and video on demand.

ME1200 IPMC, which includes IGMP and MLD protocol support, manages the IP multicast group registration. Snooping works at the Layer2 MAC level but it actually handles (Layer3) IP IGMP control messages to dedicate Layer2 MAC forwarding table.

For IPMC snooping the system needs to be in Router mode where the following two roles are defined.

- **Querier** transmits IPMC queries and is responsible for triggering multicast address determination.
- **Non-Querier** routers not selected as Querier in the same broadcast domain, such as VLAN.

IGMP/MLD Proxy

To be an IPMC proxy, the system acts as a Host/Node in reporting the joins or leaves of multicast groups towards routers. On the other hand, the system acts as a Router that collects the expected multicast group registration information from the connected hosts/nodes. In this manner IPMC control messages restrict and manage loading of the connected routers in running protocol control.

MVR

MVR is an application derived from IGMP/MLD snooping and proxy. MVR allows a subscriber on a device port to register/ unregister subscription of the multicast stream on the network-wide multicast VLAN. For example, television channels over a service provider network. It allows a single multicast VLAN to be shared on the network while subscribers remain in separate VLANs. The MVR group address required by the subscriber thus forms the VLAN trunk. To select the expected group address for an MVR VLAN requires cooperation from an IPMC profile. MVR has the following three kinds of port roles.

- **Source ports** indicate where the multicasting servers are located. Source ports are also known as Uplink ports.
- **Receiver ports** indicate where the multicast listeners are located. Receiver ports are also known as Downlink ports.
- **Inactive ports** denote that MVR operations on the designated ports are disabled.

A switch port may be a source port, a receiver port, or an inactive port in an MVR VLAN per system, and it must stay in the same port role for multiple MVR VLANs.

Each MVR VLAN works in one of the following modes.

- **Dynamic MVR** allows all IPMC control messages being traversed among the source ports. It notifies multicast routers to send the multicast data when the IPMC control message is received.
- **Compatible MVR** does not send report frames to multicast routers along with configured source ports. It is similar to the Dynamic mode in almost all other respects. In other words, Compatible MVR does not support dynamic membership joins on source ports. Routers connected wit h the source ports must be statically configured for sending the multicast stream when they cooperate with Compatible MVR.

IPMC Profile

In addition to multicast group registration that is driven by IGMP/MLD control messages, IPMC provides IPMC profile, an access control on registration. IPMC profile manages permissions in multicast registration for group tables.

An IPMC profile provides the rules for specific group addresses to decide whether or not the multicast registration should happen. The concept of an IPMC profile is similar to that of an ACL that gives permission by checking the given rules in a specific order. An IPMC profile is constructed with address range rules where the first matching condition takes effect.

IPMC Traffic Forwarding

By using IPMC snooping or proxy, the ME1200 is able to do IPv4 and/or IPv6 multicast forwarding that saves bandwidth across the network. It is also able to do access management on multicast registration by deploying the IPMC profile either in filtering utility or in throttling control. MVR deployment selects the expected group address dedicated by the IPMC profile when it is expected to restrict and prioritize certain multicast streams as they are forwarded in a proprietary VLAN trunk.

IPMC snooping/proxy and MVR can coexist to provide IPv4 and/or IPv6 multicast group registration services. However, there is priority in choosing the group address for registration between IPMC snooping/proxy and MVR.

MVR has higher priority in choosing the group address for registration because MVR should be treated as a static VLAN deployment in which the user administration must get involved. When a group address is acquired by MVR the control message regarding the specific group address is not advertised in IPMC snooping/proxy VLANs.

Limitations for IPMC Snooping, Proxy, MVR, and Profile

1. IP and MAC Hash: By using the MAC address table for forwarding IP multicast data, it is possible that two different IPMC group addresses map to the same MAC forwarding entry.

2. Unregistered Flooding Control: When the group table is full, unregistered multicast data traffic will be blocked by the unregistered flooding setting. Keep the unregistered flooding control enabled to deal with this situation.
3. Proxy for IGMPv3/MLDv2: transmits IGMPv1/IGMPv2/MLDv1 control messages upstream while the proxy is enabled. While downstream, it is able to fully handle IPMC group registration upon receiving IGMPv1/IGMPv2/IGMPv3/MLDv1/MLDv2 control messages. ME1200 does not yet fully support IGMPv3/MLDv2 in IPMC proxy.
4. SSM forwarding is not supported for all the platforms: To consider the access control resources used in chip forwarding, SSM registration information is valid on software level only.

IGMP/MLD Snooping Operation and Configuration

IPMC (IGMP/MLD) snooping is used to perform generic IP multicast group registration upon receiving IGMP/MLD control messages. IPMC protocol implementations are compliant with IGMPv3 and MLDv2 standards that are capable of handling all kinds of IPMC control messages from a connected network equipment.

To start snooping, both the global and per (IP) VLAN interface administrative controls have to be enabled. Depending on the querier election result on the VLAN, the active querier begins advertising query control messages. The hosts/nodes then respond with the join messages that include the expected group address. After the join messages are received, routers/ switches program the group table according to the collected information with a proper forwarding map. When a multicast data stream is broadcast, devices with IPMC snooping capability forward the data frame to registered group member(s) only.

IPMC Snooping

Each multicast listener reports the expected join group upon receiving the query from querier. The device is then aware of the destination port interface(s) with respect to the registered group address. When multicast data is broadcast from the server, the device only forwards the specific frame destined to the known group for the registered member(s).

The ME1200 supports both the IPv4 (IGMP) and IPv6 (MLD) multicast group registration protocols, as described in the following sections.

IGMP Snooping

IGMP is a protocol for IPv4 multicast group registration. IGMP snooping provides global administrative control and per (IP) VLAN interface management. An IGMP VLAN needs to be created and the specific IGMP VLAN enabled to start snooping IGMP control messages. The following are additional configurable IGMP VLAN interface settings regarding protocol controls.

- **Querier Election** defined in IGMP. When this option is disabled, the device will always be a Non-Querier.
- **Querier Address** IPv4 address defined as the source address used in the IP header for IGMP Querier election. When the Querier 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 default value, 192.0.2.1.
- **Compatibility** is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network.
- **Priority** of interface indicates the IGMP control frame priority level generated by the device. It can be used to prioritize the different classes of traffic.
- **RV** the robustness variable allows tuning for the expected packet loss on a network.

- **QI** the query interval is the interval between general queries sent by the querier.
- **QRI** The maximum response delay used to calculate the maximum response code inserted into the periodic general queries. This depends on the maximum response code given. The connected host/node has to respond within this interval.
- **LMQI** the last member query interval is used to guarantee the group de-registration that no more host/node requires the specific multicast address. It is also used as the contributor for protocol built-in fast leaving mechanism.
- **URI** The unsolicited report interval is the time between repetitions of a host’s initial report of membership in a group. It is used to suppress the join/report sent by the host/node.

The following table shows the basic IGMP snooping parameters and their corresponding descriptions.

Table 1 • **IGMP Snooping Parameters**

Parameters	**Description**
Global IGMP Snooping	Enable/Disable the global IGMP snooping. System starts to receive IGMP control frame when the global IGMP snooping is enabled.
Unregistered Flooding	Enable/Disable the flooding of frame destined to unregistered IPv4 group address. The flooding control takes effect only when IGMP snooping is globally enabled. When IGMP snooping is disabled, unregistered traffic flooding is always active in spite of this setting.
IGMP SSM Range	Allows SSM-aware hosts and routers to run the SSM service model for the groups in the address range. Group address in the SSM range will not allow to be advertised with EXCLUDE/BLOCK registration message.
VLAN ID	ID of the specific IGMP VLAN interface.
VLAN IGMP Snooping	Enable/Disable per (IP) VLAN IGMP snooping. System starts IGMP and does group table maintenance when per VLAN IGMP snooping is enabled.
Join Querier Election	Enable/Disable to join the IGMP querier election of the specific IGMP VLAN interface.
Querier Address	Specify the IP address used as the source address in frames generated by the device itself.
Compatibility	Specify the IGMP VLAN interface's compatibility. The choices are: IGMP-Auto, Forced IGMPv1, Forced IGMPv2, and Forced IGMPv3.
Priority	Specify the CoS priority for IGMP VLAN tagged control frame.
RV	Used as the tolerance for IGMP control frame loss.
QI	Used for the routers sending periodic general query message.
QRI	Used for the hosts as the time limit in responding the query message.
LMQI	Used for the routers to determine if any hosts expect the group address by sending specific query messages in this period of time.
URI	Used for the hosts not sending too many join/report message in this period of time.

IGMP snooping works well with the default parameters once it is globally enabled with the created and enabled VLAN interface. The rest of the functionality follows the protocol to achieve the group registration and forwarding table programming.

ME1200 IGMP snooping is disabled by default without any IGMP VLAN interface. Create and enable the IGMP VLAN interface and global administrative control to start IGMP snooping. Because IGMP snooping logical interface relies on the existing physical VLAN setting to receive and transmit protocol frames, it is important to properly configure the associated VLAN. IGMP behavior is configured by protocol parameters. Modifying these parameters requires familiarity with the IGMP standard.

The following is a quick summary of the steps.

1. Confirm unregistered flooding control is set as expected.
2. Confirm the SSM address range if it is expected to run IGMPv3 snooping for SSM capable services.
3. Create an IGMP VLAN interface and enable this interface.
4. Configure Querier Address if needed.
5. Set up Compatibility and/or Join Querier Election to force IGMP snooping in static operation (IGMPv1/IGMPv2/ IGMPv3 and/or Non-Querier) mode.
6. Set up protocol attributes (RV / QI / QRI / LMQI / URI) for IGMP to adjust protocol behaviors.
7. Assign the CoS priority for sending tagged control frames, if needed.
8. Repeat Step-3 to Step-7 for IGMP VLAN interface management.
9. Set up global IGMP snooping administrative control, if needed.
10. Save the configuration, if needed.

Default Settings and Configurable Value Range

The following table shows the default IGMP snooping settings and their configurable value range.

Table 2 • **IGMP Snooping Settings**

Configuration	Default Value	Configurable Value Range
Global IGMP Snooping	Disabled	Enabled or Disabled
Unregistered Flooding	Enabled	Enabled or Disabled
IGMP SSM Range	232.0.0.0 / 8	Valid IPv4 multicast prefix and prefix length
VLAN ID for IGMP Interface	Empty	1 ~ 4095 VLAN ID. At maximum 32 IGMP VLAN interface can be created.
VLAN IGMP Snooping	Disabled	Enabled or Disabled
Join Querier Election	Enabled	Enabled or Disabled When Disabled, the specific interface always acts as Non-Querier.
Querier Address	0.0.0.0.	Valid IPv4 unicast address
Compatibility	Auto	Auto / IGMPv1 / IGMPv2 / IGMPv3 Auto: Compatible with IGMPv1/IGMPv2/IGMPv3 IGMPv1: Forced IGMPv1 IGMPv2: Forced IGMPv2 IGMPv3: Forced IGMPv3
Priority	0	0 ~ 7 CoS value
RV	2	Packet loss tolerance count from 1 to 255
QI	125	1 - 31744 seconds
QRI	100	0 - 31744 tenths of seconds
LMQI	10	0 - 31744 tenths of seconds
URI	1	0 - 31744 seconds

IGMP Snooping Setup using ICLI

The following table shows the steps used to set up IGMP snooping using ICLI.

Table 3 • **Setting up IGMP Snooping Using ICLI**

Step	Command or Action	Purpose

1	`configure terminal`
	Example
	`# configure terminal`
	`(config)#`
		Enters global configuration mode

2	`ip igmp { ssm-range <ipv4_mcast> | unknown-flooding }`
	Example
	`(config)# ip igmp unknown-flooding`
	`(config)#`
		(Optional)
		Sets up unknown flooding or SSM range or IPv4 multicast data forwarding.

3	`ip igmp snooping vlan <vlan_list>`
	Example
	`(config)# ip igmp snooping vlan 1 (config)#`
		Creates IGMP VLAN interface(s) with specific VLAN ID or list.

4	`interface vlan <vlan_list>`
	Example
	`(config)# interface vlan 1 (config-if-vlan)#`
		Enters (IP) VLAN interface configuration mode with the specific VLAN ID or list.

5	`ip igmp snooping`
	Example
	`(config-if-vlan)# ip igmp snooping`
	`(config-if-vlan)#`
		Enables the designated (IP) VLAN interface MLD snooping function.

6	`ip igmp snooping`
	`{`
	`compatibility { auto | v1 | v2 | v3 } | last-member-query-interval <0-31744> | priority <0-7> |`
	`querier address <ipv4_ucast> |`
	`querier election |`
	`query-interval <1-31744> |`
	`query-max-response-time <0-31744> | robustness-variable <1-255> | unsolicited-report-interval <0-31744>`
	`}`
	Example
	`(config-if-vlan)# ip igmp snooping querier election`
	`(config-if-vlan)#`
		(Optional)
		Sets up IGMP VLAN interface specific configurations.

7	`exit`
	Example
	`(config-if-vlan)# exit`
	`(config)#`
		Exits from interface configuration mode and returns to global configuration mode

8	`ip igmp snooping`
	Example
	`(config)# ip igmp snooping`
	`(config)#`
		Enables the global MLD snooping function.

Table 3 • **Setting up IGMP Snooping Using ICLI**

9	`end`
	Example
	`(config)# end`
	`#`
		Returns to privileged EXEC mode

10	copy running-config startup-config
	Example
	`# copy running-config startup-config`
	`#`
		(Optional)
		Saves settings in the configuration file

IGMP Snooping Setup using Web GUI

The following steps configure IGMP snooping using the Web GUI.

1. Open the Web browser on the management platform and log in to the Web server running on the ME1200 by entering the device's IP address in the navigation bar.
2. Choose **Configuration** > **IPMC** > **IGMP Snooping** > **Basic Configuration** to display the IGMP global configuration options.
3. Enable the global IGMP Snooping mode and confirm the unregistered flooding, SSM range settings.
4. Click **Save** to keep the settings.
5. Choose **Configuration** > **IPMC** > **IGMP Snooping** > **VLAN Configuration** to display the IGMP interface configuration options.
6. Create the IGMP snooping interface(s) and assign the parameters for the IGMP VLAN interface.
7. Click **Save** to keep the settings.

Follow the numbers (1 ~ 9) in sequence to perform IGMP snooping global and interface configurations.

MLD Snooping

MLD is a protocol for IPv6 multicast group registration. MLD snooping provides global administrative control and per (IP) VLAN interface management. Except for the Querier Address, it is almost the same as "IGMP Snooping" on page 3.

The querier address used in MLD is always the IPv6 link-local address of the specific (IP) VLAN interface because MLD is a local scope protocol running for IPv6 multicast group registration. If the corresponding IP interface is not configured in the system, MLD snooping uses EUI-64 to determine the source address used in the IP header for generating MLD control messages.

The following table shows the basic MLD snooping parameters and their corresponding descriptions.

Table 4 • **MLD Snooping Parameters**

Parameter	Description
Global MLD Snooping	Enable/Disable the global MLD snooping. The system starts to receive MLD control frame when the global MLD snooping is enabled.
Unregistered Flooding	Enable/Disable the flooding of frame destined to unregistered IPv6 group address. The flooding control takes effect only when MLD snooping is globally enabled. When MLD snooping is disabled, unregistered traffic flooding is always active in spite of this setting.
MLD SSM Range	Allows the SSM-aware hosts and routers to run the SSM service model for the groups in the address range.

Table 4 • **MLD Snooping Parameters (continued)**

VLAN ID	ID of the specific MLD VLAN interface.
VLAN MLD Snooping	Enable/Disable per (IP) VLAN MLD snooping. The system starts MLD and performs group table maintenance when per VLAN MLD snooping is enabled.
Join Querier Election	Enable/Disable to join the MLD querier election of the specific MLD VLAN interface.
Compatibility	Specify the MLD VLAN interface's compatibility. The choices are: MLD-Auto, Forced MLDv1, and Forced MLDv2.
Priority	Specify the CoS priority for MLD VLAN tagged control frame.
RV	Used as the tolerance for MLD control frame loss.
QI	Used for the routers sending periodical general query message.
QRI	Used for the hosts as the time limit in responding the query message.
LMQI	Used for the routers to determine if any hosts expect the group address by sending specific query messages in this period of time.
URI	Used for the hosts not sending too many join/report messages in this period of time.

MLD snooping works well with the default parameters once it is globally enabled with created and enabled VLAN interface. The rest of the functionality follows the protocol to achieve the group registration and forwarding table programming.

Unregistered Flooding control needs to be enabled always for MLD snooping because IPv6 relies on multicast message exchanges for interface initialization. If these important messages are filtered (not to be flooded), then the connected IPv6 nodes will not function properly.

MLD snooping is disabled by default without any MLD VLAN interface. Create and enable the MLD VLAN interface and global administrative control to start MLD snooping. Because the MLD snooping logical interface relies on an existing physical VLAN setting to receive and transmit protocol frames, it is important to properly configure the associated VLAN. MLD behavior is configured by protocol parameters. Modifying these parameters requires familiarity with the MLD standard.

The following is a quick summary of the steps.

1. Confirm unregistered flooding control is set as expected. It is strongly recommended to enable unregistered flooding control for IPv6 multicast traffic.
2. Confirm SSM address range if it is expected to run MLDv2 snooping for SSM capable services.
3. Create an MLD VLAN interface and enable this interface.
4. Set up Compatibility and/or Join Querier Election to force MLD snooping in static operation (MLDv1/MLDv2 and/or Non-Querier) mode.
5. Set up protocol attributes (RV / QI / QRI / LLQI / URI) for MLD to adjust protocol behaviors.
6. Assign the CoS priority for sending tagged control frames, if needed.
7. Repeat Step-3 to Step-6 for MLD VLAN interface management.
8. Set up global MLD snooping administrative control, if needed.
9. Save the configuration, if needed.

Default Settings and Configurable Value Range

The following table shows the default MLD snooping settings and their configurable value range.

Table 5 • **Default MLD Snooping Settings**

Configuration	Default Value	Configurable Value Range
Global MLD Snooping	Disabled	Enabled or Disabled
VLAN ID for MLD Interface	Enabled	Enabled or Disabled
MLD SSM Range	ff3e:: / 96	Valid IPv6 multicast prefix and prefix length
VLAN ID for MLD Interface	Empty	1 ~ 4095 VLAN ID. At maximum 32 MLD VLAN interface can be created.
VLAN MLD Snooping	Disabled	Enabled or Disabled
Join Querier Election	Enabled	Enabled or Disabled When Disabled, the specific interface always acts as Non-Querier.
Compatibility	Auto	Auto / MLDv1 / MLDv2 Auto: Compatible with MLDv1/MLDv2 MLDv1: Forced MLDv1 MLDv2: Forced MLDv2
Priority	0	0 ~ 7 CoS value
RV	2	Packet loss tolerance count from 1 to 255
QI	125	1 - 31744 seconds
QRI	100	0 - 31744 tenths of seconds
LLQI	10	0 - 31744 tenths of seconds
URI	1	0 - 31744 seconds

MLD Snooping Setup using ICLI

The following table shows the steps used to set up MLD snooping using ICLI.

Table 6 • **Setting up MLD Snooping using ICLI**

Step	Command or Action	Purpose

1	`configure terminal`
	Example
	`# configure terminal`
	`(config)#`
		Enters global configuration mode

2	`ipv6 mld { ssm-range <ipv6_mcast> | unknown-flooding }`
	Example
	`(config)# ipv6 mld unknown-flooding`
	`(config)#`
		(Optional)
		Sets up unknown flooding or SSM range or IPv6 multicast data forwarding.

3	`ipv6 mld snooping vlan <vlan_list>`
	Example
	`(config)# ipv6 mld snooping vlan 1`
	`(config)#`
		Creates MLD VLAN interface(s) with specific VLAN ID or list.

Table 6 • **Setting up MLD Snooping using ICLI (continued)**

4	interface vlan <vlan_list> Example (config)# interface vlan 1 (config-if-vlan)#	Enters (IP) VLAN interface configuration mode with the specific VLAN ID or list.
5	ipv6 mld snooping Example (config-if-vlan)# ipv6 mld snooping (config-if-vlan)#	Enables the designated (IP) VLAN interface MLD snooping function.

6	ipv6 mld snooping
	{
	compatibility { auto | v1 | v2 } |
	last-member-query-interval <0-31744> |
	priority <0-7> |
	querier election |
	query-interval <1-31744> |
	query-max-response-time <0-31744> |
	robustness-variable <1-255> |
	unsolicited-report-interval <0-31744>
	}
	Example
	(config-if-vlan)# ipv6 mld snooping querier election
	(config-if-vlan)#
		(Optional)
		Sets up MLD VLAN interface specific configurations.

7	exit Example (config-if-vlan)# exit (config)#	Exits from interface configuration mode and returns to global configuration mode
8	ipv6 mld snooping Example (config)# ipv6 mld snooping (config)#	Enables the global MLD snooping function.
9	end Example (config)# end #	Returns to privileged EXEC mode
10	copy running-config startup-config Example # copy running-config startup-config #	(Optional) Saves settings in the configuration file

MLD Snooping Setup using Web GUI

The following steps configure MLD snooping using the Web GUI.

1. Open the Web browser on the management platform and log in to the Web server running on the ME1200 by entering the device's IP address in the navigation bar.
2. Choose **Configuration** > **IPMC** > **MLD Snooping** > **Basic Configuration** to display the IGMP global configuration options.
3. Enable the global MLD Snooping mode and confirm the unregistered flooding, SSM range settings.
4. Click **Save** to keep the settings.

5. Choose **Configuration** > **IPMC** > **MLD Snooping** > **VLAN Configuration** to display the MLD interface configuration options.
6. Create the MLD snooping interface(s) and assign the parameters for the MLD VLAN interface.
7. Click **Save** to keep the settings.

IGMP/MLD Proxy Operation and Configuration

IPMC (IGMP/MLD) proxy is used to reduce message exchanges from the IPMC control plane. IPMC proxy speaks for a set of hosts in a reporting group and it communicates with the hosts as a generic IPMC router to collect group registration information. The key idea in proxy operation is that the device will actively report the join only for the first registration (New) of a group, and the leave only for the last de-registration (Removal) of a group. The following tasks start the IPMC proxy operation.

- Enable both the global and expected (IP) VLAN interface snooping.
- Turn on proxy administrative control.
- Turn off the Join Querier Election capability on the (IP) VLAN interface.

On boot-up, the device collects the group registrations and reports the entries in the group table when the timer for the latest event reporting expires, or when the device receives a query message from querier. In other words, the device plays the role of both a host and a router at the same time. The following steps describe protocol message exchanges.

1. When 1 boots up, it reports the join for 225.5.5.5 and 228.8.8.8 to register them in the device's group table. After a while, the device sends the join for 225.5.5.5 and 228.8.8.8 group addresses.
2. Assume 2 and 3 boot up almost at the same time, but the messages from 2 come first. The new group registrations for addresses 226.6.6.6 and 227.7.7.7 are collected and registered in the device's group table. When messages from 3 arrive, the device updates the existing group registrations. After a while, the device sends the join only for 226.6.6.6 and 227.7.7.7 group addresses.
3. When 4 boots up and it sends join messages, the device updates only the existing group registrations and does not advertise the reports for join.
4. When 5 boots up and it sends join messages, the device updates only the existing group registrations and does not advertise the reports for join.
5. When the general query timer (QI) expires on a querier all the hosts receive the general query frame and respond with reports of join. The device processes the received joins from the connected listeners but filters the control frames by not forwarding them. The device also reports the joins for the recorded groups (225.5.5.5, 226.6.6.6, 227.7.7.7,and 228.8.8.8) in a local database instead.

IGMP Proxy

The IGMP proxy delegates IPv4 multicast group registration, provides global administrative controls, and cooperates with

IGMP snooping. The following table shows the basic IGMP proxy parameters and their corresponding descriptions.

Table 7 • **IGMP Proxy Parameters**

Parameter	Description
IGMP Host Proxy	Enable/Disable the global IGMP proxy. The system stops forwarding control messages to upstream directly, but when the IGMP proxy is enabled, it actively sends the group address report instead.
IGMP Leave Proxy	Enable/Disable the IGMP proxy only for group de-registration. This capability only works on IGMPv2 that provides the LEAVE message type.

Note: When global IGMP proxy is enabled, the system does proxy for both group registration and de-registration regardless of the setting for IGMP leave proxy.

MLD Proxy

The MLD proxy delegates the IPv6 multicast group registration, provides global administrative controls, and cooperates with MLD snooping. The following table shows the basic MLD proxy parameters and their corresponding descriptions.

Table 8 • **MLD Proxy Parameters**

Parameter	Description
MLD Host Proxy	Enable/Disable the global MLD proxy. The system stops forwarding control messages to upstream directly, but when the MLD proxy is enabled, it actively sends the group address report instead.
MLD DONE Proxy	Enable/Disable the MLD proxy only for group de-registration. This capability only works for MLDv1 that provides the DONE message type.

Note: When global MLD proxy is enabled, the system does proxy for both group registration and de-registration regardless of the setting for MLD leave proxy.

Configuring IGMP/MLD Proxy

Set up IPMC Snooping (see page 12) before turning on IGMP/MLD proxy on a ME1200. The following options are available for IGMP/MLD proxy:

- Leave Proxy Proxy for IGMPv2/MLDv1 leave messages only.
- Host Proxy Proxy for all kinds of IGMP/MLD control messages.

When host proxy is chosen, leave proxy is covered, but even though leave proxy becomes a redundant setting, it is still kept in configuration.

The following is a quick summary of the steps.

1. Determine whether IGMP or MLD proxy is expected.

   If IGMP proxy is expected, set up IGMP snooping first.

   If MLD proxy is expected, set up MLD snooping first.
2. Select preferred proxy option: host proxy or leave proxy.
3. Enable the specific proxy administrative control.
4. Save the configuration, if needed.

Default Settings and Configurable Value Range

The following table shows the default IGMP/MLD proxy settings and their configurable value range.

Table 9 • **IGMP/MLD Proxy Settings**

Configuration	Default Value	Configurable Value Range
IGMP Host Proxy	Disabled	Enabled or Disabled
IGMP Leave Proxy	Disabled	Enabled or Disabled
MLD Host Proxy	Disabled	Enabled or Disabled
MLD Leave Proxy	Disabled	Enabled or Disabled

IGMP/MLD Proxy Setup using ICLI

The following table shows the steps used to set up IGMP/MLD proxy using ICLI.

Table 10 • **Setting up IGMP/MLD Proxy Using ICLI**

Step	Command	Purpose

1	`configure terminal`
	Example
	`# configure terminal`
	`(config)#`
		Enters global configuration mode

2	`ip igmp host-proxy [ leave-proxy ]`
	Example
	`(config)# ip igmp host-proxy leave-proxy`
	`(config)#`
		(Optional)
		Enables IGMP host proxy or leave proxy.

3	`ipv6 mld host-proxy [ leave-proxy ]`
	Example
	`(config)# ipv6 mld host-proxy`
	`(config)#`
		(Optional)
		Enables MLD host proxy or leave proxy.

4	`end`
	Example
	`(config)# end`
	`#`
		Returns to privileged EXEC mode.

5	`copy running-config startup-config`
	Example
	`# copy running-config startup-config`
	`#`
		(Optional)
		Saves settings in the configuration file.

IGMP/MLD Proxy Setup using Web GUI

The following steps configure IGMP/MLD proxy using the Web GUI.

1. Open the Web browser on the management platform and log in to the Web server running on the ME1200 by entering the device's IP address in the navigation bar.
2. Choose **Configuration** > **IPMC** > **IGMP Snooping** > **Basic Configuration** to display the IGMP proxy configuration options.
3. Choose **Configuration** > **IPMC** > **MLD Snooping** > **Basic Configuration** to display the MLD proxy configuration options.

Note: Click the question mark at the top right for help on the configuration parameters.

MVR Operation and Configuration

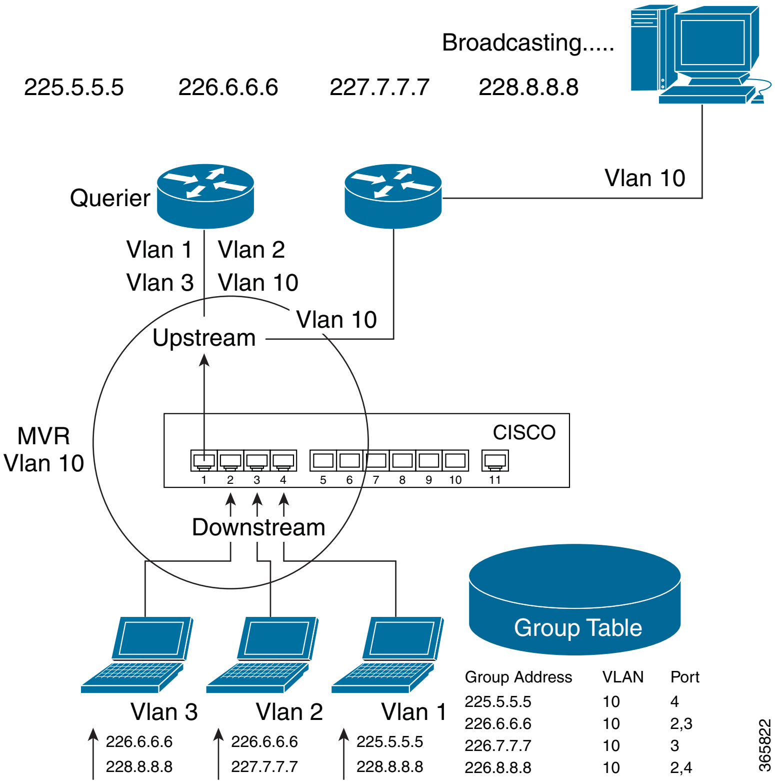
MVR is an application for IP multicast deployment. It works in a manner similar to IPMC snooping but behaves like IPMC proxy conceptually.

Static membership to MVR VLAN enables a device to obtain the group registration from downstream (receiver port) and then forward control messages upstream (source port) regardless of static VLAN management settings.

After MVR VLAN members are properly configured, an IPMC profile needs to be associated with the specific MVR VLAN to be the expected channel. For more information, see IPMC Profile Operation and Configuration (see page 40). The MVR channel is used to group a set of IP multicast streams that broadcast only on this MVR VLAN. Multicast applications can be deployed easily over an existing network connection even when the subscribers belong to different VLANs.

The following illustration shows the MVR operation over existing network connections.

Figure 19-1 ***MVR Operation***



Group Address	VLAN	Port
225.5.5.5	10	4
226.6.6.6	10	2,3
226.7.7.7	10	3
226.8.8.8	10	2,4

In this example, subscribers are attached to different VLANs (Vlan1 ~ Vlan3). However, multicast streaming services are available only to Vlan10. From a network management perspective, while it is possible to change subscriber VLAN settings as needed, this is not done typically (for example, keeping a VLAN isolated for different purpose flooding domain). Using MVR ensures that the expected multicast stream is seen by the subscribers even if they are located on different VLANs. A multicast VLAN groups a set of sources and subscribers to form a flooding domain that reduces multiple multicasting efforts from static VLANs.

The following table shows the basic MVR parameters and their corresponding descriptions.

***Table 11* • MVR Parameters**

Parameter	**Description**
Global MVR State	Enable/Disable the global MVR functionality. System starts to receive IGMP and MLD control frame when the global MVR is enabled.
MVR Interface VLAN ID	Specify the multicast VLAN ID
MVR Interface Name	Optional attribute to represent the specific MVR VLAN by using this name. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.
Interface IGMP Address	Define the IPv4 address as source address used in IP header for IGMP control frames.
Interface Mode	Specify the MVR mode of operation. Dynamic mode MVR allows dynamic MVR membership reports on source ports. Compatible mode MVR membership reports are forbidden on source ports.

Table 11 **• MVR Parameters (continued)**

Interface Tagging	Specify whether the traversed IGMP/MLD control frames are sent as untagged or tagged with MVR VID.
Interface Priority	Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The configurable values are meant to be CoS priority.
Interface LLQI	Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership.
Interface Channel Profile	When the MVR VLAN is created, select the IPMC profile as the channel filtering condition for the specific MVR VLAN. Profile selected for designated interface channel is not allowed to have overlapped permit group address used in other interface channels.
Port Role: Inactive	The designated port does not participate in MVR operations.
Port Role: Source	Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.
Port Role: 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.
Immediate Leave	Enable/Disable the fast leave on the port. When immediate leave is enabled on a port, system deletes the MAC forward entry immediately upon receiving message for group de-registration.

Note: Connecting an MVR source port directly to a management (IP) VLAN port is not recommended because the management device (PC) may not be equipped to handle VLAN tags.

Note: If a ME1200 is not deployed as an end network equipment (such as a source network equipment or an intermediate network equipment) that directly connects to the subscribers, it is strongly recommended to configure the active MVR ports as source members and turn on "Interface Tagging" for the specific MVR VLAN.

MVR runs IGMP/MLD hybrid protocol stack to provide the capability to handle both IPv4 and IPv6 multicast registrations. Therefore, it is possible and meaningful to utilize the hybrid mode IPMC profile for MVR channel application.

Complete the following tasks to deploy MVR.

- Classify the expected channels for multicast stream.
- Construct the profile for permitting the expected group addresses.
- Create a MVR VLAN with proper port roles.
- Associate the corresponding profile with this VLAN.

When MVR and IGMP/MLD snooping/proxy are enabled at the same time, only those group addresses that are not accepted by MVR are handled by IGMP/MLD snooping/proxy.

The following is a quick summary of the steps.

1. Prepare the multicast channel address ranges and construct them in IPMC profile. For more information, see IPMC Profile Operation and Configuration (see page 40).
2. Create an MVR VLAN interface and assign the expected VLAN ID. Name this MVR VLAN appropriately to ease the management effort.
3. Associate the IPMC profile configured to perform permitting expected group address registration.
4. Set up the following MVR VLAN interface parameters: IGMP Address, Mode, Tagging, Priority, and LLQI. Use default settings to ensure MVR operation.
5. Assign the MVR port role. Set the port that directly connects to subscribers as Receiver. Set the port that does not directly connect to subscribers as Source. Leave the other port Inactive because they are not expected to join the MVR operation.
6. Repeat Step-1 to Step-5 for MVR VLAN interface management.

7. Select the Immediate Leave ports that are expected to purge MAC forwarding entry as soon as possible upon receiving IGMPv2/MLDv1 leave messages.
8. Set up global MVR administrative control, if necessary.
9. Save the configuration, if needed.

Default Setting and Configurable Value Range

The following table shows the default MVR settings and their configurable value range.

***Table 12* • MVR Settings**

Configuration	Default Value	Configurable Value Range
Global MVR State	Disabled	Enabled or Disabled.
MVR Interface VLAN ID	Empty	1 ~ 4095 VLAN ID. At maximum 4 MVR VLAN interface can be created. It is also suggested not assigning the VLAN ID with existing static VLAN.
MVR Interface Name	Null string	At maximum 16 printable characters are accepted. The name string has to be unique per system.
Interface IGMP Address	0.0.0.0	Valid IPv4 unicast address.
Interface Mode	Dynamic	Dynamic or Compatible.
Interface Tagging	Tagged	Tagged or Untagged.
Interface priority	0	0 ~ 7 CoS value.
Interface LLQI	5	0 - 31744 tenths of seconds
Interface Channel Profile	Empty	Existing IPMC profile entry.
Port Role	Inactive	Inactive, Source and Receiver. The available roles are mutually exclusive for a port.
Immediate Leave	Disabled	Enabled or Disabled.

MVR Setup using ICLI

The following table shows the steps used to set up MVR using ICLI.

***Table 13* • Setting up MVR Using ICLI**

Step	Command	Purpose

1	`configure terminal`
	Example
	`# configure terminal`
	`(config)#`
		Enters global configuration mode

2	`mvr vlan <v_vlan_list> [ name <mvr_name> ]`
	Example
	`(config)# mvr vlan 10 name AN1135 (config)#`
		Creates MVR VLAN interface.

3	`mvr vlan <v_vlan_list> channel <profile_name>`
	`mvr name <mvr_name> channel <profile_name>`
	Example
	`(config)# mvr name AN1135 channel AN1135`
	`(config)#`
		Set up the interface channel by associating an existing IPMC profile.

Table 13 • **Setting up MVR Using ICLI (continued)**

<table>
<tr><td>4</td><td>mvr vlan <v_vlan_list>

{
frame priority <cos_priority> |
frame tagged |
igmp-address <v_ipv4_ucast> |
last-member-query-interval <ipmc_lmqi> |
mode { dynamic | compatible }
}
mvr name <mvr_name>
{
frame priority <cos_priority> |
frame tagged |
igmp-address <v_ipv4_ucast> |
last-member-query-interval <ipmc_lmqi> |
mode { dynamic | compatible }
}
Example
(config)# mvr name AN1135
last-member-query-interval 10 (config)#</td><td>(Optional)
Sets up MVR VLAN interface parameters for tuning MVR operations.</td></tr>
<tr><td>5</td><td>interface interface-id
Example
(config)# interface GigabitEthernet 1/4
(config-if)#</td><td>Specifies the interface on which you would like to enable MVR operation, and enters interface configuration mode.</td></tr>
<tr><td>6</td><td>mvr vlan <v_vlan_list> type { source | receiver }
mvr name <mvr_name> type { source | receiver }
Example
(config-if)# mvr vlan 10 type receiver
(config-if)#</td><td>(Optional)
Specifies the MVR port role of the designated port</td></tr>
<tr><td>7</td><td>mvr immediate-leave
Example
(config-if)# mvr immediate-leave
(config-if)#</td><td>(Optional)
Enables the immediate leave capability of the designated port</td></tr>
<tr><td>8</td><td>exit
Example
(config-if)# exit
(config)#</td><td>Exits from interface configuration mode and returns to global configuration mode.</td></tr>
<tr><td>9</td><td>mvr
Example
(config)# mvr
(config)#</td><td>(Optional)
Enables global MVR
administrative control.</td></tr>
<tr><td>10</td><td>end
Example
(config)# end
#</td><td>Returns to privileged EXEC mode.</td></tr>
<tr><td>11</td><td>copy running-config startup-config
Example
copy running-config startup-config
#</td><td>(Optional)
Saves settings in the configuration file.</td></tr>
</table>

MVR Setup using Web GUI

The following steps configure MVR using the Web GUI.

1. Open the Web browser on the management platform and log in to the Web server running on the ME1200 by entering the device's IP address in the navigation bar.
2. Choose Configuration > MVR to display the MVR configuration options. Enable the MVR administrative control to start MVR operation.
3. Click Add New MVR VLAN to create a new MVR interface. Assign the expected VLAN ID and a name for this MVR interface.
4. Associate an existing IPMC profile with this MVR VLAN as its interface channel.
5. Define the MVR VLAN interface parameters and MVR port roles.
6. Configure the expected port(s) to be immediate leave capable.

Note: Click the question mark at the top right for help information on the configuration parameters. Check the profile by clicking the "opened-eye" icon before applying the MVR VLAN channel.

IPMC Profile Operation and Configuration

IPMC profiling functions as an administrative forwarding map for IP multicasting. When a group address does not match any rule in an IPMC profile, it is dropped from multicast registration. As a result, it is important to determine the expected groups for registration in advance.

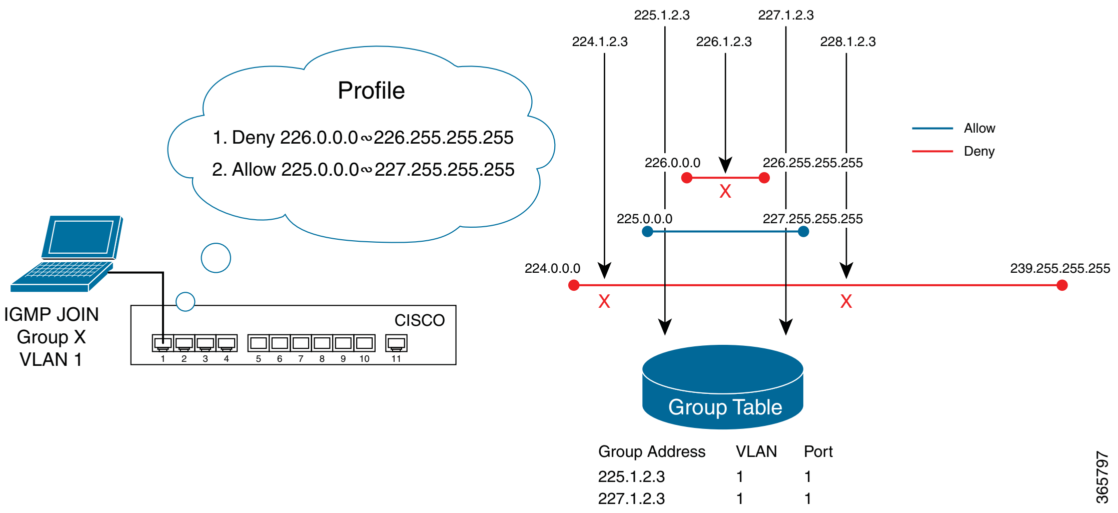
IPMC profile configuration consists of profile settings and address ranges. A profile contains filtering rules by referring to the selected address range. An address range, which may belong to different profiles, provides a set of contiguous IP multicast groups that are used for address matching.

To start using IPMC profile, the following conditions have to be met:

- The global IPMC profile administrative control has to be enabled.
- Define the address ranges for profiling. An address range can be either IPv4 multicast address or IPv6 multicast address but not a hybrid (IPv4 and IPv6 mixed) multicast address.
- Define the rules for a single profile by selecting the existing address ranges and giving corresponding actions. Smaller rule index number indicates higher priority in matching. A profile can perform access control in hybrid matching but obeys the priority order to dedicate final filtering results.
- Associate the profile with the expected application, IPMC filtering utility, and/or MVR. It depends on the application's design perspective for overlapping address tolerance: IPMC filtering utility even allows the same IPMC profile being applied on different ports, but MVR does not allow the different MVR VLANs managing the overlap groups.

When the profile is set and ready to perform filtering, every group registration request (triggered by receiving IPMC control message) starts matching to decide registration result. By inspecting the rules in the designated profile, the first matched result will be the final decision. The following figure shows the IPMC profiling operation with respect to IGMP.

Figure 19-2 ***IPMC Profiling Operation for IGMP***



Group Address	VLAN	Port
225.1.2.3	1	1
227.1.2.3	1	1

In this example, the specific profile expects to permit only the group address from 225.0.0.0 to 225.255.255.255 and 227.0.0.0 to 227.255.255.255. The first rule (index is 1) should deny group address ranges from 226.0.0.0 to 226.255.255.255, and the second rule (index is 2) should permit group address ranges from 225.0.0.0 to 227.255.255.255.

Upon receiving the JOIN message, the ME1200 starts matching the input group address with the existing rules, as shown in the following examples.

1. When 224.1.2.3 is seen, both rules are not matched so the group address is not programed into the group table.
2. When 225.1.2.3 is seen, the first rule is not matched but the second rule is matched so the group address is programed into the group table.
3. When 226.1.2.3 is seen, the first rule is matched and thus the operation stops. The first rule denies registration so the group address is not programed into the group table.
4. When 227.1.2.3 is seen, the first rule is not matched but the second rule is matched. The second rule permits registration and so the group address is programed into the group table.
5. When 228.1.2.3 is seen, both rules are not matched so the group address is not programed into the group table.

IPMC profile provides the configurable parameters used for managing profile, profile rule, and address range. The following table shows the basic IPMC profile parameters and their corresponding descriptions.

***Table 14* • IPMC Profile Parameters**

Parameter	Description
Global Profile Mode	Enable/Disable the global IPMC profile. System starts to filter based on profile settings only when the global profile mode is enabled.
Address Range Name	The name used for indexing the address entry table, and each entry has the unique name.
Start Address	The starting IPv4/IPv6 multicast group address that will be used as an address range.

Table 14 **• IPMC Profile Parameters (continued)**

End Address	The ending IPv4/IPv6 multicast group address that will be used as an address range.
Profile Name	The name used for indexing the profile table, and each entry has the unique name.
Profile Description	Additional description about the profile.
Rule Entry Name	The name used in specifying the address range for a rule. Only the existing address range entries will be chosen.
Rule Action	Indicates the learning action upon receiving the Join/Report frame that has the group address matches the address range of the rule. Permit Group address matches the range specified in the rule will be learned. Deny Group address matches the range specified in the rule will be dropped.
Log for Rule	Indicates the logging preference upon receiving the Join/Report frame that has the group address matches the address range of the rule. Enable Corresponding information of the group address, that matches the range specified in the rule, will be logged. Disable Corresponding information of the group address, that matches the range specified in the rule, will not be logged.
Next Rule	Specify next rule entry used in the same profile. When the next rule is not specified, the designated rule is added as the last entry in the profile by default. In brief, it is used to assign the priority order for rule in profile

Note: IPMC profile starts operation passively. It only provides the access control upon receiving an IPMC control message that relies on snooping, proxy, and MVR administration.

Without any profile, address range, and rule entry, the IPMC profile is disabled by default. Create address ranges and profiles, and associate expected ranges as rules used in a specific profile to set up an IPMC profile. When IPMC access control is required, enable global IPMC profile to start filtering. The following is a quick summary of the steps.

1. Create address range with proper entry name.
2. Repeat Step-1 for expected address range management.
3. Create profile with proper entry name.
4. Set up additional descriptions for designated IPMC profile entry, if necessary.
5. Associate an address range entry with designated IPMC profile entry as a profile rule.
6. Set up action and log preference for the rule.
7. Assign the priority order of the rule in the designated IPMC profile entry, if necessary.
8. Repeat Step-3 ~ Step-7 for profile management.
9. Set up global IPMC profile administrative control, if necessary.
10. Save the configuration, if needed.

Always check the precedence of rules in a profile before applying the specific profile.

Default Setting and Configurable Value Range

The following table shows the default IPMC profile settings and their configurable value range.

Table 15 **• IPMC Profile Settings**

Configuration	Default Value	Configurable Value Range
Global Profile Mode	Disabled	Enabled or Disabled.

Table 15 • **IPMC Profile Settings (continued)**

Address Range Name	Null string	At maximum 16 printable characters are accepted. The name string has to be unique per system. There are at most 128 address range entries to be created.
Start Address	Empty	Valid IPv4 or IPv6 multicast address. It has to be the same version address as ‘End Address’
End Address	Empty	Valid IPv4 or IPv6 multicast address. It has to be the same version address as ‘Start Address’
Profile Name	Null string	At maximum 16 printable characters are accepted. The name string has to be unique per system. There are at most 64 profile entries to be created.
Profile Description	Null string	At maximum 64 printable characters are accepted.
Rule Entry Name	Null string	Any existing address range configured in the system.
Rule Action	Deny	Permit or Deny
Log for Rule	Disabled	Enabled or Disabled
Next Rule	Least priority (Last rule in profile)	Any existing rule in the specific IPMC profile.

IPMC Profile Setup using ICLI

The following table shows the steps used to set up IPMC profile using ICLI.

Table 16 • **Setting up IPMC Profile Using ICLI**

Step	Command	Purpose

1	`configure terminal`
	Example
	`# configure terminal`
	`(config)#`
		Enters global configuration mode.

2	`ipmc profile`
	Example
	`(config)# no ipmc profile`
	`(config)#`
		(Optional)
		Enable/Disable global IPMC profiling function.

3	`ipmc range range-name start-ip-multicast-address end-ip-multicast-address`
	Example
	`(config)# ipmc range Video 227.3.3.3 228.123.123.123`
	`(config)# ipmc range Data 238.0.0.0 239.255.255.255`
	`(config)# ipmc range Audio 225.1.1.1 225.222.222.222`
	`(config)# ipmc range Game 226.0.0.0 226.255.255.255`
	`(config)#`
		Define the expected address ranges.

4	`ipmc profile profile-name`
	Example
	`(config-if)# ipmc profile AN1135 (config-if)#`
		Specifies the name of IPMC profile entry on which access control is enabled, and enters IPMC profile configuration mode.

Table 16 **• Setting up IPMC Profile Using ICLI (continued)**

5	`description`
	Example
	`(config-ipmc-profile)# description Demonstration for Configuration Guides AN1135`
	`(config-ipmc-profile)#`
		(Optional)
		Add additional notes for describing the specific profile.

6	`range range-name {deny | permit} [log] [next range-name]`
	Example
	`(config-ipmc-profile)# range Audio permit log`
	`(config-ipmc-profile)# range Data permit`
	`(config-ipmc-profile)# range Video permit next Data`
	`(config-ipmc-profile)#`
		Arrange and configure rules for the specific profile.

7	`end`
	Example
	`(config-ipmc-profile)# end`
	`#`
		Returns to privileged EXEC mode.

8	`show ipmc profile [profile-name] [detail]`
	Example
	`# show ipmc profile`
	`IPMC Profile is currently disabled,`
	`please enable profile to start filtering.`
	`Profile: AN1135 (In IGMP Mode)`
	`Description: Demonstration for Configuration Guides AN1135`
	`HEAD-> Audio (Permit the following range and log the matched entry) Start Address: 225.1.1.1`
	`End Address: 225.222.222.222`
	`NEXT-> Video (Permit the following range) Start Address: 227.3.3.3`
	`End Address: 228.123.123.123`
	`NEXT-> Data (Permit the following range) Start Address: 238.0.0.0`
	`End Address: 239.255.255.255`
	`#`
		Confirm the configured IPMC profile filtering conditions.

9	`copy running-config startup-config`
	Example
	`# copy running-config startup-config`
	`#`
		(Optional)
		Saves settings in the configuration file.

Note Use `no` command to negate configured settings. Use the show ipmc profile detail command to display the matching conditions in detail to help in understanding the filtering result of a specific address.

IPMC Profile Setup using Web GUI

The following steps configure IPMC profile using the Web GUI.

1. Open the Web browser on the management platform and log in to the Web server running on the ME1200 by entering the device's IP address in the navigation bar.

2. Choose **Configuration** > **IPMC Profile** > **Address Entry** to display the configuration page for setting the profile address range. The following illustration shows the IPMC profile address range configurations in the Web GUI. Follow the numbers (1 ~ 5) in sequence to perform configuration.
3. Choose **Configuration** > **IPMC Profile** > **Profile Table** to display the configuration page for setting the profile entry. The following illustration shows the IPMC profile entry configurations in the Web GUI. Follow the numbers (1 ~ 7) in sequence to perform configurations. In the last operation 7', system redirects the configuration page to the designated profile's rule configuration page in next step.
4. Click **Add Last Rule** to create a rule for this profile as the last entry. Select the available address range using Entry Name and assign the Action and Log preferences. Multiple range entries are permitted but they must be unique in a profile. Optional control buttons (in operation) allow creating, removing, or re-prioritizing the rules associated with this profile. The following illustration shows the IPMC profile rule configurations in the Web GUI. Follow the numbers (1 ~8) in sequence to perform profile rule configurations and checking the precedence of rules in this profile. In the last operations '7 ~ 8", system pops the new window for displaying profile rule status.

Note: Click the question mark at the top right for help information on the configuration parameters

Note: Always remember to enable global IPMC profile administrative control before applying expected filter operations.

IGMP/MLD Utility Operation and Configuration

The IPMC provides four additional utilities for static controls on "IPMC Snooping" on page 3.

1. **Filtering** restricts group registration based on the given profiling access control. Only the allowed groups will be registered. For information about profiling access controls, see "IPMC Profile Operation and Configuration" on page 18.
2. **Throttling** limits the number of groups registered, based upon the throttling value.
3. **Fast Leave** deletes the MAC forward entry regardless of the protocol confirmation when a message for leaving a group is received.
4. **Router Port** statically configures a specific port as upstream, which means it connects to another IPMC router(s).

The following table shows the basic IPMC utility parameters and their corresponding descriptions.

***Table 17* • IPMC Utility Parameters**

Parameter	Description
Filtering Profile	Specify the profile to be used in filtering group registration.
Throttling Value	Specify the maximum number of group registrations.
Fast Leave	Performs deleting MAC forward entry immediately upon receiving message for group de-registration.
Router Port	Specify the interface is connected with another IPMC router(s).

Each utility need to be configured per-port because they are used to enhance IGMP/MLD snooping and IPMC performs Layer2 snooping. The following are some examples of typical use.

- The filtering utility can be used to limit the multicast address forwarding for a specific port.
- The throttling utility can be used to restrict the amount of multicast address registration on a certain port to save group table resource.
- The fast leave utility can be used to speed up the group purging for a better multicast streaming experience.
- The router port utility can be used to manually specify the upstream for IPMC control plane.

The following is a quick summary of the steps.

1. Define the purpose and investigate the possible results of applying these utilities.
2. Set up the IPMC profile first to use the filtering utility. For more information, see "IPMC Profile Operation and Configuration" on page 18.
3. Associate the expected IPMC profile to be filtered on a specific port, if required.

Note: Filtering from a hybrid mode profile applied on either IGMP or MLD snooping port(s) is possible, but not filtering from a pure IGMP profile applied on a MLD snooping port and vice versa.

4. Assign the throttling number to limit the amount of group registration on a specific port, if required.
5. Enable the fast leave for immediate purging MAC forwarding entry on a specific port, if required.
6. Select the upstream connection (where a multicast router is attached) on a specific port, if required.
7. Save the configuration, if needed.

Default Setting and Configurable Value Range

The following table shows the default IPMC utility settings and their configurable value range.

***Table 18* • IPMC Utility Settings**

Configuration	Default Value	Configurable Value Range
Filtering Profile	Empty	Existing IPMC profile entry.
Throttling Value	Unlimited	1-10 number of group registration.
Fast Leave	Disabled	Enabled or Disabled.
Router Port	Disabled	Enabled or Disabled.

IGMP/MLD Utility Setup using ICLI

The following table shows the steps used to set up IGMP/MLD utilities using ICLI.

***Table 19* • Setting up IGMP/MLD Utilities Using ICL**

Step	Command	Purpose

1	`configure terminal`
	Example
	`# configure terminal`
	`(config)#`
		Enters global configuration mode.

2	`interface interface-id`
	Example
	`(config)# interface GigabitEthernet 1/4`
	`(config-if)#`
		Specifies the interface on which you are using the IPMC utility, and enters interface configuration mode.

3	`ip igmp snooping filter <word16>`
	`ipv6 mld snooping filter <word16>`
	Example
	`(config-if)# ip igmp snooping filter AN1135`
	`(config-if)#`
		(Optional)
		Set up filtering feature.

4	`ip igmp snooping max-groups <1-10> ipv6 mld snooping max-groups <1-10>`
	Example
	`(config-if)# ipv6 mld snooping max-groups 3`
	`(config-if)#`
		(Optional)
		Set up throttling feature.

Table 19 • **Setting up IGMP/MLD Utilities Using ICL (continued)**

5	`ip igmp snooping immediate-leave ipv6 mld snooping immediate-leave`
	Example
	`(config-if)# ipv6 mld snooping immediate-leave`
	`(config-if)#`
		(Optional)
		Set up fast leave feature.

6	`ip igmp snooping mrouter ipv6 mld snooping mrouter`
	Example
	`(config-if)# ip igmp snooping mrouter`
	`(config-if)# ipv6 mld snooping mrouter`
	`(config-if)#`
		(Optional)
		Set up router port feature

7	`end`
	Example
	`(config-if)# end`
	`#`
		Returns to privileged EXEC mode.

8	`copy running-config startup-config`
	Example
	`# copy running-config startup-config`
	`#`
		(Optional)
		Saves settings in the configuration file.

IPMC Profile Setup using Web GUI

The following steps configure IGMP/MLD utilities using the Web GUI.

1. Open the Web browser on the management platform and log in to the Web server running on the ME1200 by entering the device's IP address in the navigation bar.
2. Choose **Configuration** > **IPMC** > **IGMP Snooping** > **Port Filtering Profile** to display the configuration options for the IGMP port filtering utility.
3. Choose **Configuration** > **IPMC** > **IGMP Snooping** > **Basic Configuration** to display the configuration options for the IGMP port throttling, fast leave, and router port utilities. The following illustration shows the IGMP utility configurations in the Web GUI. Follow the numbers (1 ~ 7) in sequence to perform IGMP snooping utility configurations.
4. Choose **Configuration** > **IPMC** > **MLD Snooping** > **Port Filtering Profile** to display the configuration options for the MLD port filtering utility.
5. Choose **Configuration** > **IPMC** > **MLD Snooping** > **Basic Configuration** to display the configuration options for the MLD port throttling, fast leave, and router port utilities. Follow the numbers (1 ~ 7) in sequence to perform MLD snooping utility configurations.

Note: Click the question mark at the top right for help information on the configuration parameters. Check the profile by clicking the "opened-eye" icon before applying the port filtering.

IPMC Configuration Examples

Complete the following tasks to be able to start managing the IPMC functionality.

1. Prepare a computer

   Ensure the computer is equipped with a (USB) RS-232 connector and NIC card.

   – Install Linux OS uBuntu LTS version on this computer. For information about installation steps, see http://www.ubuntu.com/download/desktop/install-ubuntu-desktop.

   – Add the minicom software package

```
$ sudo apt-get install minicom
```

- Configure the minicom software

```
(Find out the expected group to access the expected serial adapter in the
computer. In this case, 'dialout' is the group name and there are at least
two serial adapters available: 'ttyS0' and ' ttyUSB0'.)
$ ls -alp /dev | grep tty
…
crw-rw----1 root dialout4,64 Nov 13 19:17 ttyS0
…
crw-rw----1 root dialout4,73 Nov 1 15:53 ttyS9 crw-rw----1 root dialout
188,  0 Nov 1 15:53 ttyUSB0
…
(Use command "usermod" to add your Ubuntu user as a member of group
'dialout' if user is not in the specific group. To check whether user belongs
to the group 'dialout', use command "id" to identify.)
$ id me1200
uid=2000 gid=1000 groups=1000
$ sudo usermod -a -G dialout me1200
$ id me1200
uid=2000 gid=1000 groups=1000,20(dialout
)
(Setup USB RS-232 adaptor as minicom's default connection, for
example.)
$ sudo minicom -s
(Select 'Serial port setup' after executing command.)
+-----[configuration]------+
| Filenames and paths|
| File transfer protocols|
| Serial port setup|
| Modem and dialing|
| Screen and keyboard|
| Save setup as dfl|
| Save setup as..|
| Exit|
| Exit from Minicom|
+-------------------------+
(Change the serial port setting as below to meet the serial configuration.)
+---------------------------------------------------------------
--------+
| A-Serial Device: /dev/ttyUSB0
|
| B -Lockfile Location: /var/lock
|
| C-Callin Program:
|
| D-Callout Program:
|
| E-Bps/Par/Bits: 115200 8N1
|
| F -Hardware Flow Control : No
|
| G -Software Flow Control : No
|
|
|
|  Change which setting?
|
+---------------------------------------------------------------

--------+
| Screen and keyboard|
| Save setup as dfl|
| Save setup as..|
| Exit|
| Exit from Minicom|
+--------------------------+

(Select 'Save setup as dfl' after changing serial port setting is done.)
```

2. Prepare a network equipment that supports IPMC Profile/Snooping/Proxy and MVR.
3. Connect the computer and the equipment with serial cable and network cable, and ensure both of them are running.
4. Confirm or set up IP configuration of equipment by using the minicom application, and then make sure the IP communication is active between equipment and computer by using PING.

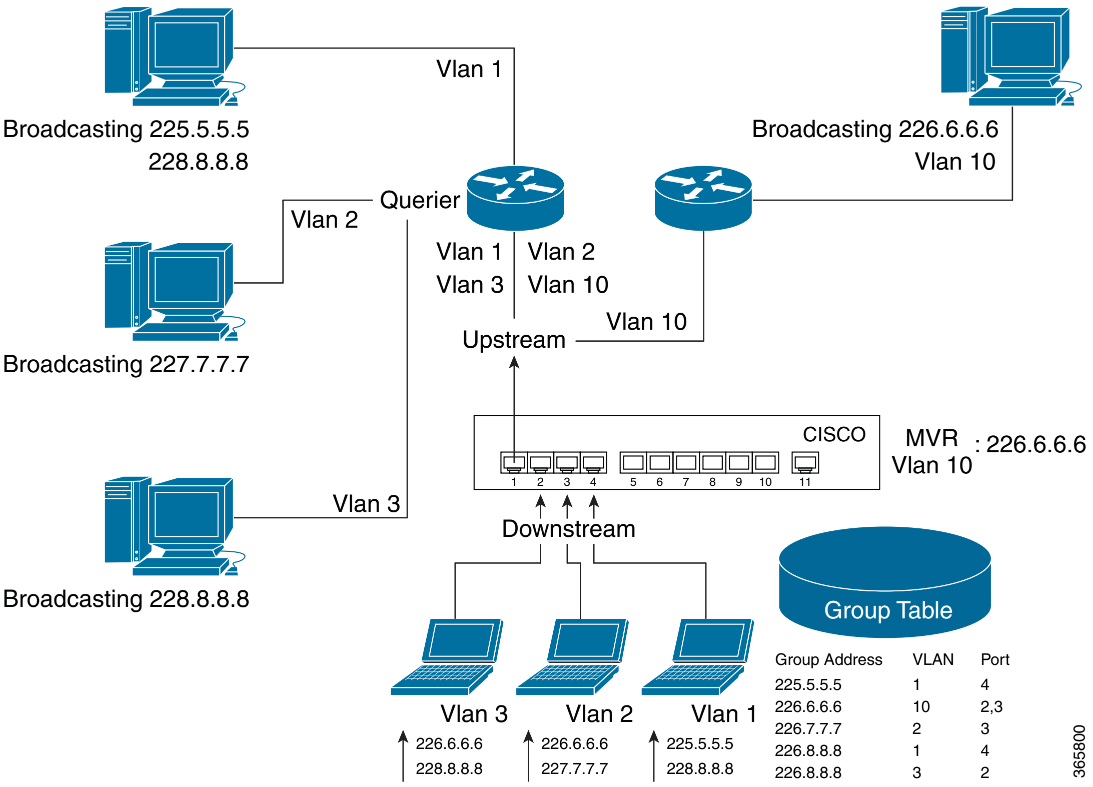
   (In this case, the IP address of the computer is '192.0.2.88' while

   the IP address of the equipment is '192.0.2.1'.)

```
$ ifconfig
eth0Link encap:EthernetHWaddr 00:10:60:76:b4:a5
inet addr:192.0.2.88 Bcast:192.0.2.255Mask:255.255.255.0 inet6 addr:
fe80::210:60ff:fe76:b4a5/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500Metric:1
RX packets:793 errors:0 dropped:0 overruns:0 frame:0
TX packets:791 errors:1 dropped:0 overruns:0 carrier:0 collisions:0
txqueuelen:1000
RX bytes:89148 (89.1 KB)TX bytes:89606 (89.6 KB)
$ minicom
Welcome to minicom 2.7
OPTIONS: I18n
Compiled on Jan 1 2014, 17:13:19. Port /dev/ttyUSB0
Press CTRL-A Z for help on special keys
Username: admin
Password:
# show interface vlan
VLAN1
LINK: 00-01-c1-00-c2-70 Mtu:1500 <UP BROADCAST RUNNING MULTICAST> IPv4:
192.0.2.1/24 192.0.2.255
IPv6: fe80::201:c1ff:fe00:c270/64 <UP RUNNING>
# ping ip 192.0.2.88
PING server 192.0.2.88, 56 bytes of data.
64 bytes from 192.0.2.88: icmp_seq=0, time=10ms
64 bytes from 192.0.2.88: icmp_seq=1, time=0ms
64 bytes from 192.0.2.88: icmp_seq=2, time=0ms
64 bytes from 192.0.2.88: icmp_seq=3, time=0ms
64 bytes from 192.0.2.88: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
#
```

The following topology illustration is used to demonstrate the examples, which assume the device boots up with its default configuration. It also demonstrates the final group registration results after completing the examples.

Figure 19-3 IPMC Configuration Example Topology



Group Address	VLAN	Port
225.5.5.5	1	4
226.6.6.6	10	2,3
226.7.7.7	2	3
226.8.8.8	1	4
226.8.8.8	3	2

Deploy IPMC Profile for Filtering Multimedia Stream

The IPMC profile is set primarily to provide the access control in multicast learning and thus managing forwarding. Therefore we expect only the address ranges from 225.0.0.0 to 228.255.255.255 will be handled by ME1200. We will then create an IPMC profile and use this profile for filtering IGMP group registration.

```
# configure terminal
(config)# ipmc range SuperSet 225.0.0.0 228.255.255.255 (config)# ipmc profile
Demonstration
(config-ipmc-profile)# range SuperSet permit log
(config-ipmc-profile)# exit
(config)# ipmc profile
(config)# do show ipmc profile detail
IPMC Profile is now enabled to start filtering. Profile: Demonstration (In IGMP
Mode) Description:
HEAD-> SuperSet (Permit the following range and log the matched entry) Start
Address: 225.0.0.0
End Address: 228.255.255.255
IGMP will deny matched address between [224.0.0.0 <-> 224.255.255.255]
IGMP will permit and log matched address between [225.0.0.0 <-> 228.255
.255.255]
IGMP will deny matched address between [229.0.0.0 <-> 239.255.255.255] MLD will
deny matched address between [ff00:: <-> ffff:ffff:ffff:ffff:
ffff:ffff:ffff:ffff]
(config)# interface *
(config-if)# ip igmp snooping filter Demonstration
(config-if)# exit
```

```
(config)# ip igmp snooping vlan 1 (config)# interface vlan 1
(config-if-vlan)# ip igmp snooping
(config-if-vlan)# exit
(config)# ip igmp snooping
(config)# do show ip igmp snooping detail
IGMP Snooping is enabled to start snooping IGMP control plane.
Multicast streams destined to unregistered IGMP groups will be flooding
.
Switch-1 IGMP Interface Status
IGMP snooping VLAN 1 interface is enabled.
Querier status is ACTIVE (Administrative Control: Join Querier-Election
)
Startup Query Interval: 25 seconds; Startup Query Count: 1
Querier address is not set and will use system's IP address of this int erface.
Active IGMP Querier Address is 0.0.0.0
PRI:0 / RV:2 / QI:125 / QRI:100 / LMQI:10 / URI:1
RX IGMP Query:0 V1Join:0 V2Join:0 V3Join:0 V2Leave:0
TX IGMP Query:0 / (Source) Specific Query:0
IGMP RX Errors:0; Group Registration Count:0
Compatibility:IGMP-Auto / Querier Version:Default / Host Version: Default
Older Version Querier Present Timeout: 0 second Older Version Host Present
Timeout: 0 second (config)# end
#
```

Snooping IPv4 Multicast Registration in Different VLAN

Assume that the connected hosts separate into different VLAN for management purposes. VLAN configuration and IGMP snooping need to be set up at the same time.

```
# configure terminal
(config)# vlan 2
(config-vlan)# exit (config)# vlan 3 (config-vlan)# exit
(config)# interface GigabitEthernet 1/4 (config-if)# switch mode access
(config-if)# switch access vlan 1
(config-if)# interface GigabitEthernet 1/3 (config-if)# switch mode access
(config-if)# switch access vlan 2
(config-if)# interface GigabitEthernet 1/2 (config-if)# switch mode access
(config-if)# switch access vlan 3
(config-if)# interface GigabitEthernet 1/1 (config-if)# switch mode trunk
(config-if)# switch trunk native vlan 1
(config-if)# swtich trunk allowed vlan 1,2,3 (config-if)# exit
(config)# ip igmp snooping vlan 2 (config)# ip igmp snooping vlan 3 (config)#
interface vlan 1-3 (config-if-vlan)# ip igmp snooping (config-if-vlan)# exit
(config)# ip igmp snooping
(config)# do show ip igmp snooping detail
IGMP Snooping is enabled to start snooping IGMP control plane.
Multicast streams destined to unregistered IGMP groups will be flooding
.
Switch-1 IGMP Interface Status
IGMP snooping VLAN 1 interface is enabled.
Querier status is ACTIVE (Administrative Control: Join Querier-Election
)
Querier Up time: 3190 seconds; Query Interval: 91 seconds
Querier address is not set and will use system's IP address of this int erface.
Active IGMP Querier Address is 10.9.52.198
PRI:0 / RV:2 / QI:125 / QRI:100 / LMQI:10 / URI:1
RX IGMP Query:0 V1Join:0 V2Join:0 V3Join:0 V2Leave:0
TX IGMP Query:3 / (Source) Specific Query:0
```

```
IGMP RX Errors:0; Group Registration Count:0
Compatibility:IGMP-Auto / Querier Version:Default / Host Version: Default
Older Version Querier Present Timeout: 0 second Older Version Host Present
Timeout: 0 second IGMP snooping VLAN 2 interface is enabled.
Querier status is ACTIVE (Administrative Control: Join Querier-Election
)

Startup Query Interval: 24 seconds; Startup Query Count: 1
Querier address is not set and will use system's IP address of this int erface.
Active IGMP Querier Address is 0.0.0.0
PRI:0 / RV:2 / QI:125 / QRI:100 / LMQI:10 / URI:1
RX IGMP Query:0 V1Join:0 V2Join:0 V3Join:0 V2Leave:0
TX IGMP Query:1 / (Source) Specific Query:0
IGMP RX Errors:0; Group Registration Count:0
Compatibility:IGMP-Auto / Querier Version:Default / Host Version: Default
Older Version Querier Present Timeout: 0 second Older Version Host Present
Timeout: 0 second IGMP snooping VLAN 3 interface is enabled.
Querier status is ACTIVE (Administrative Control: Join Querier-Election
)
Startup Query Interval: 24 seconds; Startup Query Count: 1
Querier address is not set and will use system's IP address of this int erface.
Active IGMP Querier Address is 0.0.0.0
PRI:0 / RV:2 / QI:125 / QRI:100 / LMQI:10 / URI:1
RX IGMP Query:0 V1Join:0 V2Join:0 V3Join:0 V2Leave:0
TX IGMP Query:1 / (Source) Specific Query:0
IGMP RX Errors:0; Group Registration Count:0
Compatibility:IGMP-Auto / Querier Version:Default / Host Version: Default
Older Version Querier Present Timeout: 0 second Older Version Host Present
Timeout: 0 second (config)# end
#
```

Deploy MVR and IGMP Snooping at The Same Time

Create another IPMC profile and a new MVR VLAN to deploy an MVR VLAN over the existing network with permitting gaming group in range 226.0.0.0/8 (226.0.0.0 ~ 226.255.255.255). In this example, MVR VLAN ID is set as 10 and this MVR VLAN only forwards the multicast stream in the channel to subscribers.

```
# configure terminal
(config)# ipmc range Game 226.0.0.0 226.255.255.255 (config)# ipmc profile Game
(config-ipmc-profile)# range Game permit log
(config-ipmc-profile)# exit
(config)# ipmc profile
(config)# do show ipmc profile detail

IPMC Profile is now enabled to start filtering. Profile: AN1135 (In IGMP Mode)
Description: Demonstration for Configuration Guides AN1135
HEAD-> Audio (Permit the following range and log the matched entry) Start
Address: 225.1.1.1
End Address : 225.222.222.222
NEXT-> Video (Permit the following range) Start Address: 227.3.3.3
End Address : 228.123.123.123
NEXT-> Data (Permit the following range) Start Address: 238.0.0.0
End Address : 239.255.255.255
IGMP will deny matched address between [224.0.0.0 <-> 225.1.1.0]
IGMP will permit and log matched address between [225.1.1.1 <-> 225.222
.222.222]
IGMP will deny matched address between [225.222.222.223 <-> 227.3.3.2] IGMP
will permit matched address between [227.3.3.3 <-> 228.123.123.123
]
IGMP will deny matched address between [228.123.123.124 <-> 237.255.255
.255]
IGMP will permit matched address between [238.0.0.0 <-> 239.255.255.255
]
MLD will deny matched address between [ff00:: <-> ffff:ffff:ffff:ffff:
ffff:ffff:ffff:ffff]
Profile: Demonstration (In IGMP Mode) Description:
HEAD-> SuperSet (Permit the following range and log the matched entry)
Start Address: 225.0.0.0
End Address : 228.255.255.255
IGMP will deny matched address between [224.0.0.0 <-> 224.255.255.255] IGMP
will permit and log matched address between [225.0.0.0 <-> 228.255
.255.255]
IGMP will deny matched address between [229.0.0.0 <-> 239.255.255.255] MLD will
deny matched address between [ff00:: <-> ffff:ffff:ffff:ffff:
ffff:ffff:ffff:ffff]
Profile: Game (In IGMP Mode) Description:
HEAD-> Game (Permit the following range and log the matched entry) Start
Address: 226.0.0.0
End Address : 226.255.255.255
IGMP will deny matched address between [224.0.0.0 <-> 225.255.255.255] IGMP
will permit and log matched address between [226.0.0.0 <-> 226.255
.255.255]
IGMP will deny matched address between [227.0.0.0 <-> 239.255.255.255] MLD will
deny matched address between [ff00:: <-> ffff:ffff:ffff:ffff:
ffff:ffff:ffff:ffff]
(config)# mvr vlan 10 name Game (config)# mvr name Game channel Game (config)#
mvr
(config)# do show mvr detail
MVR is now enabled to start group registration. Switch-1 MVR-IGMP Interface
Status
IGMP MVR VLAN 10 (Name is Game) interface is enabled. Querier status is IDLE
( Forced Non-Querier )
Querier Expiry Time: 255 seconds
IGMP address is not set and will use system's IP address of this interf ace.
Control frames will be sent as Tagged
PRI:0 / RV:2 / QI:125 / QRI:100 / LMQI:5 / URI:1
RX IGMP Query:0 V1Join:0 V2Join:0 V3Join:0 V2Leave:0
TX IGMP Query:0 / (Source) Specific Query:0
IGMP RX Errors:0; Group Registration Count:0
Port Role Setting:
Inactive Port: Gi 1/1,Gi 1/2,Gi 1/3,Gi 1/4,Gi 1/5,Gi 1/6,Gi 1/7,Gi 1/8, Gi
1/9,G 1/1,G 1/2
Interface Channel Profile: Game (In IGMP Mode) Description:
HEAD-> Game (Permit the following range and log the matched entry) Start
Address: 226.0.0.0
End Address: 226.255.255.255
Switch-1 MVR-MLD Interface Status
MLD MVR VLAN 10 (Name is Game) interface is enabled. Querier status is IDLE (
Forced Non-Querier )
Querier Expiry Time: 255 seconds
MLD address will use Link-Local address of this interface. Control frames will
be sent as Tagged
PRI:0 / RV:2 / QI:125 / QRI:100 / LMQI:5 / URI:1
RX MLD Query:0 V1Report:0 V2Report:0 V1Done:0
TX MLD Query:0 / (Source) Specific Query:0
MLD RX Errors:0; Group Registration Count:0
Port Role Setting:
Inactive Port: Gi 1/1,Gi 1/2,Gi 1/3,Gi 1/4,Gi 1/5,Gi 1/6,Gi 1/7,Gi 1/8, Gi
1/9,G 1/1,G 1/2
```

```
Interface Channel Profile: Game (In IGMP Mode) Description:
HEAD-> Game (Permit the following range and log the matched entry) Start
Address: 226.0.0.0
End Address: 226.255.255.255 (config)# end
#
```

Note In this topology, group address destined to addresses not included in the SuperSet will be flooding. Data destined to 225.5.5.5 from VLAN 1 will be forwarded to port 4. Data destined to 226.6.6.6 from VLAN 10 will be forwarded to port 2 & 3. Data destined to 227.7.7.7 from VLAN 2 will be forwarded to port 3. Data destined to 228.8.8.8 from VLAN 1 will be forwarded to port 4. Data destined to 228.8.8.8 from VLAN 3 will be forwarded to port 2.

CHAPTER 20

HTTPS Configuration

This document demonstrates how to set up HTTPS for secure communication between http client (usually a web browser) and http server using ICLI commands.

Using ICLI as the management interface requires a serial console connection between the device and management platform. No network connection is required to use ICLI, but the terminal emulator software has to be installed.

The HTTPS functionality is meant for secure communication between a browser (management console) and a web server (switch). The included self-signed certificate may trigger a browser warning that the certificate is not issued by a trusted source. The certificate upload mechanism in the switch software enables use of a trusted third-party certificate.

Understanding HTTPS

HTTPS (Hypertext Transfer Protocol Secure) is a method for securing HTTP data transfer over a TCP/IP network. It adds the security capabilities of SSL/TLS to standard HTTP communications between an HTTP client (usually a web browser) and an HTTP server (usually a web server). The main motivation for HTTPS is to prevent man-in-the-middle attacks or eavesdropping.

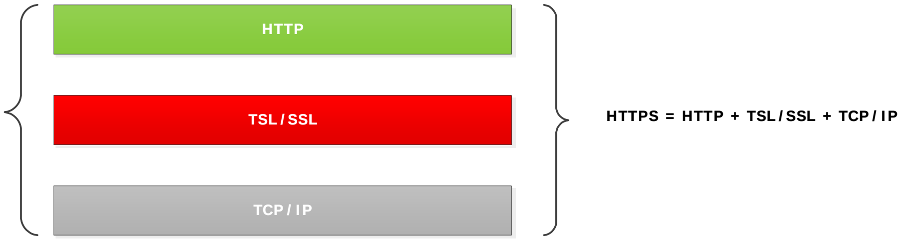
Restrictions for HTTPS

Per HTTP communication models, the host (web server) addresses and port numbers are necessarily part of the underlying TCP/IP protocols. HTTPS cannot protect their disclosure but encrypts the content of the HTTP data (payload)- that means an eavesdropper can infer the IP address, domain name, and port number of the web server but not the content of the applications.

HTTPS Working Model

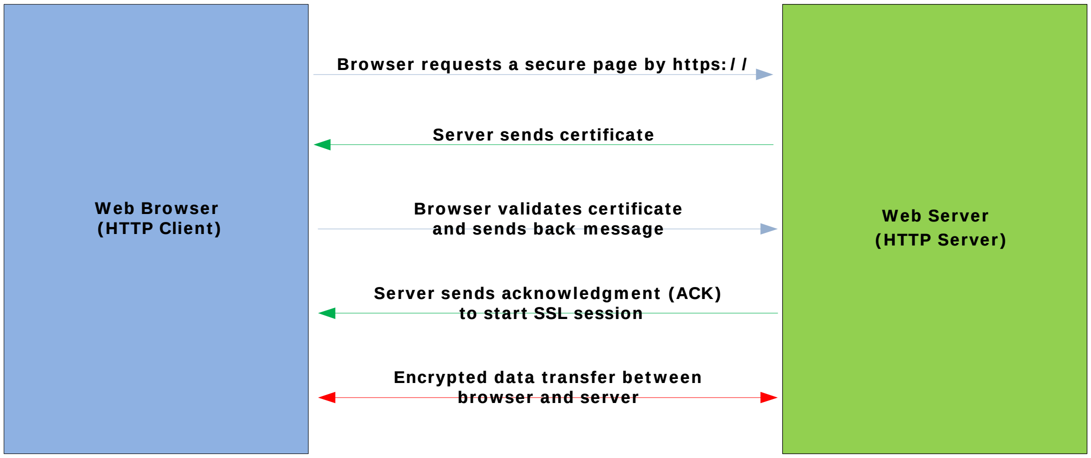
- **Protocol layering**- HTTPS is a mechanism to layer HTTP on top of SSL/TLS and to add securities capabilities to HTTP application.

Figure 1 • **Protocol Layering**



- **Authentication** - The web browser requires a server certificate from the web server before an SSL/TLS connection is established. An SSL/TSL connection is required before HTTPS data transfer can commence.
- **Encryption**- Once an SSL connection is established, data transfer is encrypted with a public key provided by a security certificate.

Figure 2 • **Encryption**


Web Browser
(HTTP Client)
Browser requests a secure page by https: / /
Server sends certificate
Browser validates certificate
and sends back message
Server sends acknowledgment (ACK)
to start SSL session
Encrypted data transfer between
browser and server
Web Server
(HTTP Server)

Configuration Prerequisites

This section lists the prerequisites for configuring and/or monitoring operations on devices using the management platform.

- Computer with (USB) RS-232 connector and NIC card
- Terminal emulator software that supports the serial port
- Serial port parameters, as follows:
  - Baud rate: 115200
  - Data bits: 8 bits
  - Stop bit: 1 bit
  - Flow control: Disable
  - Parity check: None

Configuring HTTPS

HTTPS is enabled by default in ME1200 switches. A web browser can access a switch at https://ip-address-of-switch/. This section provides guidelines for changing configurations for a switch booted-up using the default settings.

To configure HTTPS using ICLI, connect a serial RS-232 cable with the switch while the terminal console software is running on host.

HTTPS Default Setting and Configurable Value Range

The following table provides details of the HTTPS default setting and configurable value range.

Table 1 • **HTTPS Default Setting and Configurable Value Range**

Configuration	Default Value	Configurable Value
Mode	Enabled	Enabled, Disabled
Automatic Redirect	Disabled	Enabled, Disabled
Certificate Maintain	None	None, Delete, Upload, Generate
Certificate Algorithm	RSA	RSA, DSA
PassPhrase	None	A string pattern
Certificate Upload	Web Browser	Web Browser, URL
Certificate Status	N/A	Non-configurable

Setting up HTTPS using ICLI

Setting up HTTPS is a multi step process, as described.

Enabling HTTPS

```
Enters global configuration mode
# configure terminal
Enables the HTTPS
(config)# ip http secure-server
HTTPS mode is enabled and the browser can request a secure data via
https://
```

Automatically Redirecting the Web Browser to the HTTPS Mode

```
Enters global configuration mode
# configure terminal
Enables automatic redirect
(config)# ip http secure-redirect
HTTPS automatic redirect is enabled
```

Maintaining Certificate

```
Disable HTTPS
(config)# no ip http secure-server
Delete HTTPS certificate
(config)# ip http secure-certificate delete
HTTPS certificate is now deleted
```

Generating a New Certificate to Replace the Current Certificate

```
Disable HTTPS
(config)# no ip http secure-server
Generate HTTPS certificate with RSA or DSA
To generate certificate with RSA algorithm:
(config)# ip http secure-certificate generate RSA
```

or

```
To generate certificate with DSA algorithm.
(config)# ip http secure-certificate generate DSA
HTTPS certificate is now generated
```

Uploading a third-party Certificate Externally to Replace the Current One

```
Disable HTTPS
(config)# no ip http secure-server
Upload certificate from tftp or http servers, below is an example for
uploading a named 3rd-party certificate, https_server_certificate.pem
from tftp server whose IP address is 10.0.0.123
(config)# ip http secure-certificate upload \
tftp://10.0.0.123/https_server_certificate.pem
HTTPS certificate is now uploaded
```

Note Disable HTTPS before uploading, generating, or deleting a certificate. Enable HTTPS after completing the process.

CHAPTER 21

Configuring Y.1564

This document describes the Y.1564 test feature supported by the switch software running on the carrier Ethernet switches. The document explains the basic concepts of Y.1564 test and describes how to execute Y.1564 test on the carrier Ethernet switches. It provides examples on how to configure and execute the Y.1564 test through either the web Graphical User Interface (GUI) or through the Industrial Command Line Interface (ICLI) management interfaces. This description applies to both eCos- and Linux-based software packages.

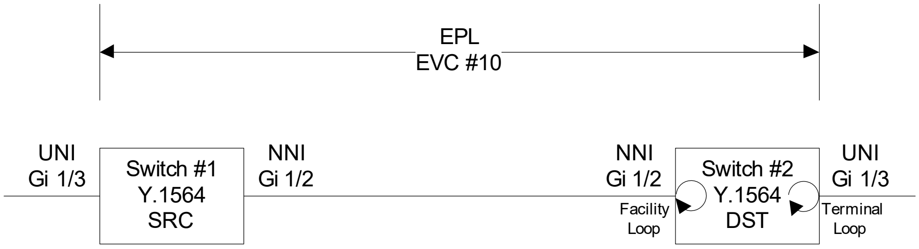
Quick Configuration

The following sections describe how to perform a quick Y.1564 test of an EPL (Ethernet Private Line) Ethernet Virtual Connection (EVC) between two switches connected directly (as shown in the following illustration) through CLI commands.

The Y.1564 software supports only single-ended traffic, that is, test traffic originates and terminates on the same switch. This switch is referred to as the local end or SRC. The switch on which the partner UNI is located is referred to as the remote end or DST. It is up to the operator to configure this switch to loop traffic so that the traffic that arrives at NNI or is about to depart UNI at the remote end is looped back to the local end.

In the following illustration, GigabitEthernet (Gi) 1/3 is the User Network Interface (UNI) and Gi 1/2 is the Network-to-Network Interface (NNI) for both switches.

Figure 1 • **Y.1564 Setup**



For an OAM unaware test, the remote end (Switch #2) is configured to loop all the traffic arriving on the EVC at NNI. This is a so-called Facility MAC-Loop in the EVC domain (leftmost circular arrow). With this setup, only the UNI-to-NNI path is tested.

For an OAM-aware test, a full UNI-to-UNI test is performed and EVC at the remote end's UNI is looped. This is known as a terminal OAM-loop in the EVC domain (rightmost circular arrow).

Creating EVC

First create the EVC on which Y.1564 tests are to be executed. For the sake of UNI-to-UNI tests, the same EVC configuration must be applied to both the SRC and the DST switch. For UNI-to-NNI tests, the remote end does not need an EVC configuration, only a facility loop.

The following commands create the EVC on which Y.1564 tests are executed.

```
# Disable STP on UNI ports or traffic may be discarded before
# it enters UNI, especially if there's no link on UNI.
# We also disable it on NNI, because we know from the VLAN configuration
# below, that no other frames can exit or enter that port, so there will
# be no loops, even though MSTP might put the EVC's IVID in discarding.
interface GigabitEthernet 1/2,3
 no spanning-tree

# Exclude UNI/NNI ports from all VLANs and set PVID to an unused VLAN
# NNI is an S-port
interface GigabitEthernet 1/2
 switchport hybrid native vlan 4095
 switchport hybrid allowed vlan none
 switchport hybrid port-type s-port
 switchport mode hybrid

# UNI is a C-port
interface GigabitEthernet 1/3
 switchport hybrid native vlan 4095
 switchport hybrid allowed vlan none
 switchport hybrid port-type c-port
 switchport mode hybrid

# Enable classification based on VLAN tag on NNI interface
interface GigabitEthernet 1/2
 qos trust tag
 qos map tag-cos pcp 0 dei 0 cos 0 dpl 0
 qos map tag-cos pcp 0 dei 1 cos 0 dpl 1
 qos map tag-cos pcp 1 dei 0 cos 1 dpl 0
 qos map tag-cos pcp 1 dei 1 cos 1 dpl 1

# EVC configuration
# Add EVC 10 using S-VID 1000, disable learning
evc 10 vid 1000 ivid 1000 interface GigabitEthernet 1/2 policer none

# Add ECE 1 mapping all frames on UNI to EVC 10. Use policer #12
# Only add the policer on SRC switch.
evc ece 1 interface GigabitEthernet 1/3 outer-tag add dei-mode dp evc 10 policer 12 cos 4

# Configure policer #12
evc policer 12 enable cir 10000 cbs 50000 eir 6000 ebs 20000
```

Creating Y.1564 Test Profile on Switch #1

Ensure to create two test profiles on Switch #1. One of the profile uses simulated customer traffic and the other uses Y.1731 LBM and DMM traffic. The test profiles are named as profile-OAM-unaware and profile-OAM-aware, respectively.

- For profile-OAM-unaware, select simulated customer traffic, allow up to 30% frame loss, and only enable the CIR test. All the other parameters are kept at their default values.

```
# Create a test profile named profile-OAM-unaware.
# Use simulated customer traffic, allow up to 30 permille frame loss,
# only enable CIR test
y1564 profile profile-OAM-unaware
 traffic-type customer-simulated
 acceptable-flr 30
 no eir-test
 no traffic-policing-test
 no performance-test
```

- For profile-OAM-aware, select dst-oam-aware and Y.1731 OAM traffic, set the MEG level to 7, allow up to 30% frames loss, and only enable the CIR test. All the other parameters are kept at their default values.

```
# Create a test profile named profile-OAM-aware
# Set ‘DST is OAM aware’, use Y.1731 LBM and DMM traffic, MEG level 7,
# allow up to 30 permille frame loss, only enable CIR test
y1564 profile OAM-aware
 dst-oam-aware
 traffic-type oam
 meg-level 7
 acceptable-flr 30
 no eir-test
 no traffic-policing-test
 no performance-test
```

Creating Traffic Test Loop on Switch #2

To match the two test profiles on Switch #1, also create two traffic test loops on Switch #2. For the OAM unaware test profile using customer simulated traffic, create a facility loop of type MAC-loop on the NNI port of the EVC (port 3) of Switch #2 on EVC 10.

```
# Create Traffic Test Loop instance #1 for OAM unaware test.
# Facility MAC-loop on NNI in the EVC domain with EVC ID 10.
# Keep it disabled to begin with.
traffic-test-loop 1 type mac-loop interface GigabitEthernet 1/2 direction facility
domain evc 10 admin-state disabled
```

For the OAM-aware test (using Y.1731 LBM and DMM traffic), an OAM-loop must be created on the EVC. It is a terminal loop on the UNI port.

```
# Create Traffic Test Loop instance #2 for OAM-aware test.
# Terminal OAM-loop on UNI in the EVC domain with EVC ID 10.
# Keep it disabled to begin with.
# NOTICE: The 'warning-ignore' flag is not supported on all products.
# If supported, it is required in order to prevent VSC7418 to print
# a warning and deny the command to take effect when the loop gets enabled.
# The reason it would print a warning is that it's not only the
# EVC that is looped, but actually the whole UNI, so that all
# services running on this UNI will be affected.
traffic-test-loop 2 type oam-loop level 7 interface GigabitEthernet 1/3 direction
terminal domain evc 10 admin-state disabled warning-ignore
# The following causes the loop to also look for OAM behind a possible C-tag.
traffic-test-loop 2 subscriber all
```

Running Y.1564 Tests on Switch #1

Connect an Ethernet cable between Gi 1/2 of the two switches.

Running OAM Unaware Test

Before running the test, use the following ICLI commands to enable the Facility MAC-loop on Switch #2.

```
# Enable traffic test loop instance 1 (facility MAC-loop in EVC domain)
traffic-test-loop 1 admin-state enable
```

Execute the following command to start the test on Switch #1 and show the report once it is done.

```
# Start an Y.1564 test using profile-OAM-unaware on EVC 10.
# Default is to start all ECEs defined in that EVC.
# Save the report in a file called report-OAM-unaware.
y1564 start report-OAM-unaware profile profile-OAM-unaware evc 10

# Check y1564 test progress
show y1564 report

Report Name                       Created                    Status
--------------------------------  -------------------------  -----------------
report-OAM-unaware                1970-01-01T00:12:18+00:00  In progress

# Check y1564 test progress again
show y1564 report

Report Name                       Created                    Status
--------------------------------  -------------------------  -----------------
report-OAM-unaware                1970-01-01T00:12:18+00:00  Succeeded
# show y1564 report report-OAM-unaware
****************************************************************************
* Y.1564 SAM Test
****************************************************************************
Software configuration:
  Version                     : <Software Version>
  Board                       : <Hardware Board>
  Build date                  : 2017-10-24T15:41:46+02:00

Profile configuration:
  Profile name                : profile-OAM-unaware
  Description                 :
  Measurement type            : Single-ended (DST loops traffic)
  DST is OAM aware            : No
  Test traffic type           : Simulated customer traffic
  Test traffic SMAC           : Use port MAC
  Delay measurement type      : Y.1731 1DM
  MEG Level                   : 7
  Dwell time                  : 500 msecs
  Frame size                  : 512 (EMIX=d)
  User-defined frame size     : 2000 bytes
  CIR configuration test      : Enabled
  EIR configuration test      : Disabled
  Traffic policing test       : Disabled
  Service performance test    : Disabled
  Acceptable FLR              : 30 permille
  Acceptable FTD              : Check disabled
  Acceptable FDV              : Check disabled

Report configuration:
  Report name                 : report-OAM-unaware
  Description                 :
  Peer MAC                    : 00-00-00-00-00-01
  EVC ID                      : 10
  EVC VLAN ID                 : 1000
  ECE IDs on EVC              : 1
  ECE IDs under test          : 1 (Auto)

Configuration for UNI interface GigabitEthernet 1/3:
  Link state                  : Down
  Speed                       : 1000 Mbps
  MTU                         : 10240 bytes
  MAC                         : 00-01-c1-00-00-03

Configuration for NNI interface GigabitEthernet 1/2:
  Link state                  : Up
  Speed                       : 1000 Mbps
  MTU                         : 10240 bytes

Configuration for Policer ID 12:
  ECE use count               : 1/1
  CIR/EIR                     : 10.000/6.000 Mbps
  CBS/EBS                     : 50000/20000 bytes
  Rate Type                   : Layer 2 (data)
  Policer Type                : Color Aware

Configuration for ECE ID 1:
  Under test                  : Yes
  Matching                    :
    Outer VLAN Tag Type       : Any
    Inner VLAN Tag Type       : Any
    Frame Type                : Any
  Actions                     :
    Tx Lookup                 : VID
    Policer ID                : 12
    Tag Pop Count             : 0
    CoS                       : 4
    Drop Precedence           : From basic classification
    Egress Outer Tag PCP Mode : Classified
  Resolutions                 :
    UNI interface             : GigabitEthernet 1/3 (Auto)
    PCP of NNI Outer Tag      : 4
    VLAN ID                   : 1 (Auto)
    PCP                       : 0 (Auto)
    Green flow                : DEI = 0 (Auto)
    Yellow flow               : Inactive (Unable to generate yellow flow into policer,
because the UNI port's default QoS settings mark the frame green)
    DSCP                      : N/A
    Frame size                : 516 bytes
    Frame                           : 00 00 00 00 00 01 00 00  01 c1 00 03 81 00 00 01
                                     : 88 80 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                                     : 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                                     : 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                              : ...
                                    : 00 00 00 00 00 00 00 0a  00 00 00 01 xx xx xx xx

Test Results table legend:
  UNI Ingr ECE                : The ECE ID for which the rest of this row
                                 pertains
  UNI Egr ECE                 : The ECE that counts looped traffic for the
                                 corresponding UNI Ingr ECE
  UNI Ing CoS                  : Class of Service that UNI ingress traffic on
                                this ECE maps to
  Color/Step #                : Color of frame flow (G = Green, Y = Yellow)
                                and step number in CIR configuration test
  Color                       : Color of frame flow
  Under Test                      : Indicates whether this ECE was selected to be
                               tested when the test was initiated
  UNI Ingr, Requested         : Requested traffic rate on UNI, in Line Rate
```

```
                               (L1) and Data Rate (L2)
  UNI Ingr, Applied              : Hardware doesn't always support the requested
                               rate. This is the rate that hardware
                              : tells software it supports given the
                                requested rate
  UNI Ingr, In-service           : The rate and frame count after policing on the
                               UNI. This is the rate supposed to egress NNI.
                              : Notice, that this rate may be somewhat lower
                                than what is expected given the policer's
                                       : configuration and applied rate. The reason for
                              this is that the hardware may burst up
                              : to eight frames per flow in order to achieve
                                a given rate. This may not pose a problem
                              : if the policer's CBS/EBS is configured to
                                absorb these bursts, that is, set to values
                              : that are at least eight times the test frame
                                size. If not, green frames may be painted
                              : yellow/red and yellow frames may be painted
                                red (discarded) when passing through the
                              : policer. The net-effect is in-service rates
                                that are lower than anticipated, and the
                              : yellow counters may count on pure green
                                traffic at CIR or below. If this situation
                                occurs,
                                   : a warning will be displayed under the relevant
                              policer's configuration section in this
                              : report.
  UNI Egr                            : Actual NNI->UNI frame count after looping (may
                              be 0 if counted on another ECE)
  Frame Loss                     : Percentage of frames lost between UNI ingress
                               and UNI egress
  Status                      : PASS, SKIP, FAIL or empty if not under test

Delay Measurements table legend:
  UNI Ing CoS                 : Class of Service that UNI ingress traffic on
                                the ECEs under test maps to
  UNI Egr CoS                        : Class of Service that counts looped DM traffic
                              for the corresponding UNI ingress CoS
  Under Test                  : Indicates whether an ECE mapping to
                               this ingress CoS is under test
  Step #                      : Step number in CIR configuration test
  DM Tx                            : Number of transmitted Delay Measurement frames
  DM Rx                       : Number of received Delay Measurement frames
  Min/Avg/Max Delay           : Minimum, average, and maximum delay seen on the DM frames
  Min/Avg/Max Delay Var.         : Minimum, average, and maximum delay variation seen on
the DM frames
  Status                      : PASS or FAIL - only for CoSs under test

Overall execution status:
  Started at                  : 1970-01-01T00:12:18+00:00
  Ended at                    : 1970-01-01T00:13:00+00:00
  Status                      : Succeeded

************************************************** CIR configuration test
Configuration:
  Duration per step           : 10 seconds
  Delay meas. interval        : 500 msecs
  Step count                  : 4

Status:
  Started at                  : 1970-01-01T00:12:18+00:00
  Ended at                    : 1970-01-01T00:13:00+00:00
  Status                      : Succeeded
```

```
Test Results:
---- ---- --- ------ ----- ----------------- ----------------- --------------
UNI  UNI  UNI Color/ Under UNI Ingr (L1/L2)  UNI Ingr (L1/L2)  UNI Ingr (L1/L2)  UNI Ingr
UNI Egr      Frame  Status
Ingr Egr  Ing Step # Test  Requested         Applied           In-service
In-service                Loss
ECE  ECE  CoS             [Mbps]           [Mbps]           [Mbps]           [Frames]
[Frames]     [%]
---- ---- --- ------ ----- ----------------- ----------------- -----------------
------------ ----------- ------ ------
   1    1   4 G/1    Yes          2.596/2.500       2.593/2.497       2.591/2.494
6044         6044   0.00 PASS
   1    1   4 Y/1    Yes                                              0.000/0.000
0            0        PASS
   1    1   4 G/2    Yes          5.193/5.000       5.192/4.999       5.191/4.997
12106        12106   0.00 PASS
   1    1   4 Y/2    Yes                                              0.000/0.000
0            0        PASS
   1    1   4 G/3    Yes          7.790/7.500       7.764/7.475       7.762/7.472
18104        18104   0.00 PASS
   1    1   4 Y/3    Yes                                              0.000/0.000
0            0        PASS
   1    1   4 G/4    Yes        10.387/10.000      10.290/9.907      10.287/9.903
23992        23992   0.00 PASS
   1    1   4 Y/4    Yes                                              0.000/0.000
0            0        PASS

Delay Measurements:
--- --- ------ ----- -------- -------- ----------------- ----------------- ------
UNI UNI Step # Under   DM Tx    DM Rx      Min/Avg/Max       Min/Avg/Max       Status
Ing Egr       Test                  Delay             Delay Var.
CoS CoS              [Frames] [Frames] [usecs]           [usecs]
--- --- ------ ----- -------- -------- ----------------- ----------------- --
  0          1 No            0        0
  1          1 No            0        0
  2          1 No            0        0
  3          1 No            0        0
  4   4      1 Yes          20       20       6/6/7             0/0/0 PASS
  5          1 No            0        0
  6          1 No            0        0
  7          1 No            0        0
  0          2 No            0        0
  1          2 No            0        0
  2          2 No            0        0
  3          2 No            0        0
  4   4      2 Yes          20       20       6/6/7             0/0/0 PASS
  5          2 No            0        0
  6          2 No            0        0
  7          2 No            0        0
  0          3 No            0        0
  1          3 No            0        0
  2          3 No            0        0
  3          3 No            0        0
  4   4      3 Yes          20       20       6/6/7             0/0/0 PASS
  5          3 No            0        0
  6          3 No            0        0
  7          3 No            0        0
  0          4 No            0        0
  1          4 No            0        0
  2          4 No            0        0
  3          4 No            0        0
  4   4      4 Yes          20       20       6/6/7             0/0/0 PASS
  5          4 No            0        0
  6          4 No            0        0
  7          4 No           0        0

********************* Overall Result *********************************
  Ended at                    : 1970-01-01T00:13:00+00:00
  Status                      : Succeeded
****************************************************************************
```

Running OAM-Aware Test

For the OAM-aware test, the peer-MAC address must be specified when starting the Y.1564 test. The peer MAC address is the MAC address of the switch port on which the OAM-loop is created. In this example, it is the MAC address of UNI (Gi 1/3) of Switch #2.

First enable the correct traffic loop on Switch #2:

```
# Disable the facility traffic test loop that got enabled in the previous test
traffic-test-loop 1 admin-state disable
# Enable the terminal traffic test loop
traffic-test-loop 2 admin-state enable
```

Then, start the test on Switch #1 and keep polling until it is complete.

```
# Start an Y.1564 test using profile-OAM-aware on EVC 10.
# Default is to start all ECEs defined in that EVC.
# Save the report in a file called report-OAM-aware.
# Since it's an OAM-aware test, we need to specify the remote
# end's MAC address on the looping interface. This can be found
# on Switch #2 by following the steps outlined in chapter 7.1.
y1564 start report-OAM-aware profile profile-OAM-aware evc 10 peer-mac 00-01-c1-00-b5-33

# Check y1564 test progress
show y1564 report

Report Name                       Created                    Status
--------------------------------  -------------------------  -----------------
report-OAM-unaware                1970-01-01T00:12:18+00:00  Succeeded
report-OAM-aware                  1970-01-01T00:12:21+00:00  In progress

# Check y1564 test progress again
show y1564 report

Report Name                       Created                    Status
--------------------------------  -------------------------  -----------------
report-OAM-unaware                1970-01-01T00:12:18+00:00  Succeeded
report-OAM-aware                  1970-01-01T00:12:21+00:00  Succeeded
```

Understanding ITU-T Y.1564

ITU-T Y.1564 (Or sometimes called Y.156sam or EtherSAM - Ethernet Service Activation Methodology) is a Quality of Service (QoS) and network performance ITU-T Ethernet-based service test methodology.In the following, it is simply referred to as "Y.1564".

Y.1564 is an out-of-service testing procedures test service turn-up, installation, and troubleshooting of Ethernet-based services with the goal of assuring and verifying committed Service Level Agreement (SLA) performances.

Prior to Y.1564 the most widely used testing tool to assess performance of Ethernet-based services was IETF RFC 2544 (RFC 2544 test is also supported by CE switches and CEServices software. Refer to [ENT-AN1111]), which was created to evaluate the performance characteristics of network devices in a lab. It includes throughput, burstability (back-to-back test), frame loss and latency tests and is being used for Ethernet-networks globally. However, it does not include all required measurements such as packet delay variation, QoS measurement with bandwidth profiles (CIR, CBS, EIR, EBS and Color mode) and multiple concurrent service levels. Contrary to RFC2544, Y.1564 allows simultaneous testing of multiple Ethernet services and measures if they qualify to the committed SLA attributes. On top of that it also validates the different QoS mechanisms provisioned in the network to prioritize the different service types - allowing service providers faster deployment and easier service and network troubleshooting.

Y.1564 defines test streams (or "flows") with service attributes aligned to the Metro Ethernet Forum (MEF) definitions. These test flows can be classified using various mechanisms such as 802.1q VLAN, 802.1ad, DSCP, and class of service (CoS) profiles and map to Ethernet virtual connections (EVCs). These services are defined at the UNI level with different frame and bandwidth profiles such as committed information rate (CIR), and excess information rate (EIR).

Y.1564 is a Carrier Ethernet Switch feature supported by both hardware (Carrier Ethernet Switch with ViSAA architecture) and software (CEServices software running on the internal CPU of the switch chip). The test flows are generated and injected by the switch's hardware at UNI ingress at the source switch, and are looped back at the destination switch by a hardware-based traffic test loop, and the test flows are gathered again at UNI egress at the source switch. Nano-second accurate delay measurement is made possible with the hardware-based timestamp engine.

As stated, Y.1564 is an out-of-service testing methodology, meaning that the service under test (EVC) will be taken down during the testing, so that traffic arriving at the local ends of the UNI that gets classified to the EVC will be discarded. This is taken care of by the Y.1564 software. If the remote end is a Cisco-branded switch, the 'traffic-test-loop' functionality takes care of taking the EVC out of service, provided the traffic test loop is created on an EVC. Third-party switches may have different means to take an EVC out of service. Notice, that on Cisco-branded switches, there is no guarantee that non-EVC loops prevent EVC traffic from entering NNI from the remote end towards the local end. This may or may not lead to Y.1564 tests to fail, depending on the nature of the traffic, the configuration of the ECEs and which ECEs are under test.

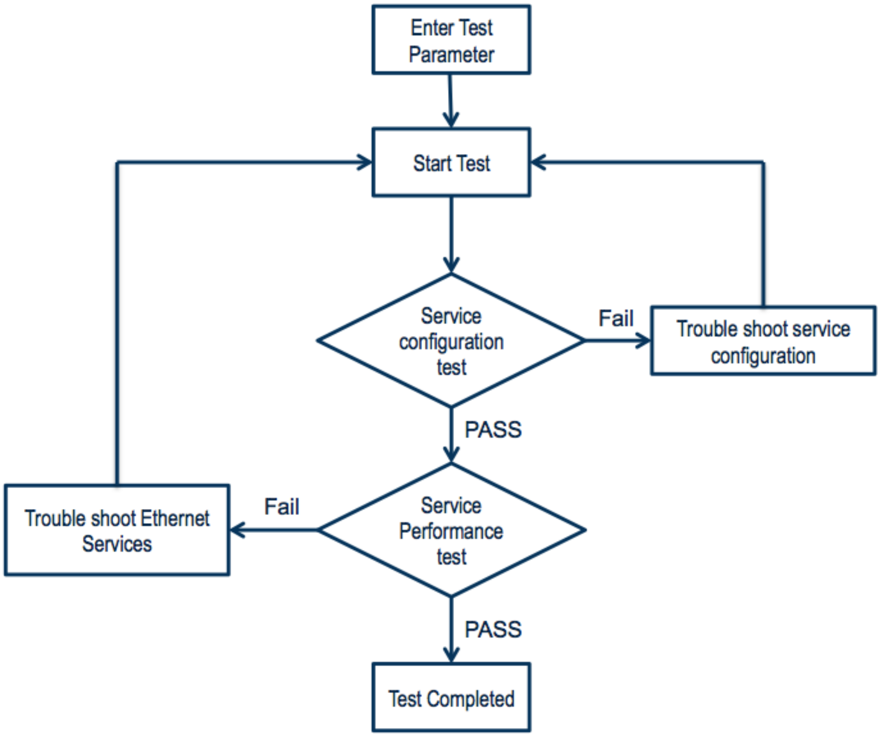
Y.1564 Test Types

Y.1564 test methodology has two main objectives:

- to validate that each Ethernet-based services is correctly configured
- to validate that the quality of the services as delivered to the end-user

Therefore, the methodology comprises service configuration test and a service performance test as shown in the following illustration.

Figure 2 • **High-level Service Activation Methodology**


Enter Test Parameter
Start Test
Service configuration test
Fail
Trouble shoot service configuration
PASS
Service Performance test
Fail
Trouble shoot Ethernet Services
PASS
Test Completed

The goal of the service configuration test is to validate that the services are configured as intended. Service configuration test comprises of CIR test, EIR test, and traffic policing tests. Those tests together with service performance test are described individually in the following sections.

For each of the tests, a green and yellow flow rate is computed for each ECE under test. If the resulting, summarized line utilization rate (L1) becomes greater than the UNI link speed, the test will be skipped.

In the following, the terms such as color-aware and color-blind are used for the policers. Please refer to Appendix A for a description of policer types.

CIR Configuration Test

If CIR is zero, the test is skipped. If the policer is color-aware and it is impossible to create a flow that is green when it hits the policer, the test is skipped along with the explanation.

If the policer is color-blind and it is possible to create a flow that is green when it hits the policer, use that flow. If the policer is color-blind and it is impossible to create a flow that is green when it hits the policer, use a yellow flow.

Step load is used for the CIR configuration test to gradually reach the CIR. When step count is configured to four (default) a test flow transmits at 25%, 50%, 75%, and finally 100% of CIR.

For each step, the received IR, FLR, FTD, and FDV is measured and compared against the SAC, and the test fails if either of these do not meet the SAC. If 100% of CIR has been reached successfully, the CIR test succeeds. Only green flows have their FLR compared to the SAC, since it is not possible to fail on yellow flows.

EIR Configuration Test

If EIR is zero or the policer is of type Single Leaky Bucket (SLB), the test is skipped.

The EIR configuration test can be performed on both color-aware and color-blind policers. Depending on the color awareness, the EIR configuration test is done.

Policer is Color-Aware

Unless CIR is 0, a color-aware test requires both a green and a yellow flow. If CIR is 0, only a yellow flow is required. If the required frame colors can not be created, then the test is skipped along with an explanation.

The green flow has rate of CIR and the yellow flow has a rate of EIR.

For the green flow only, measure IR, FLR, FTD, and FDV and compare it to the SAC. If it meets the SAC, the test passes, otherwise it fails. IR and FLR for the yellow flow are computed for reporting purposes, but is not matched against the SAC, and therefore can't make the test fail.

Policer is Color-Blind

If the policer is color-blind, only one flow is generated. Since, with respect to policer, it is equally good to use a green and a yellow flow towards the policer, either colored flow works. A green flow is chosen over a yellow flow.

The rate of the flow is CIR + EIR.

If the ingress flow is green, measure IR and FLR and compare it to the SAC. If the ingress flow is yellow, measure IR and FLR only for reporting purposes, since the test can fail on yellow frames.

Also measure FTD and FDV and compare it to the SAC. If the SAC is met, the test passes, otherwise it fails.

Traffic Policing Test

If the policer is color-aware, the following algorithm from the ITU-T Y.1564 recommendation applies:

```
If EIR < 20% * CIR
   Green  = 100% * CIR
   Yellow =  25% * CIR + 100% * EIR
Else
   Green  = 100% * CIR
   Yellow = 125% * EIR
EndIf
```

If CIR is non-zero, it must be possible to create a flow that hits the policer as green. Otherwise the test is skipped.

If the resulting yellow frame rate is non-zero, it must be possible to create a flow that hits the policer as yellow. Otherwise the test is skipped.

Notice that even though EIR is zero, it must be possible to create a yellow flow for the test not to be skipped.

If the policer is color-blind, only one flow is generated. The rate of that flow is given by the following algorithm from the ITU-T Y.1564 recommendation:

```
If EIR < 20% * CIR
   Rate = 125% * CIR + 100% * EIR
```

```
Else
   Rate = 100% * CIR + 125% * EIR
EndIf
```

As per policer, it is equally good to use a green and a yellow flow towards the policer, either colored flow will work. A green flow will be chosen if it's possible to create it.

If the ingress flow is green, measure IR and FLR and compare it to the SAC. If the ingress flow is yellow, measure IR and FLR only for reporting purposes, since the test can fail on yellow frames.

Also measure FTD and FDV and compare it to the SAC. If the SAC is met, the test passes, otherwise it fails.

Service Performance Test

Service performance test validates the quality of the services over time up to 24 hours.

If CIR is zero, the test is skipped.

If the policer is color-aware and it is impossible to create a flow that is green when it hits the policer, then the test is skipped along with a description of why.

If the policer is color-blind and it is possible to create a flow that is green when it hits the policer, then use that flow. If the policer is color-blind and it is impossible to create a flow that is green when it hits the policer, then use a yellow flow.

The received IR, FLR, FTD, and FDV is measured and compared against the SAC, and the test fails if either of these don't meet the SAC. Only green flows have their FLR compared to the SAC, since it is not possible to fail on yellow flows.

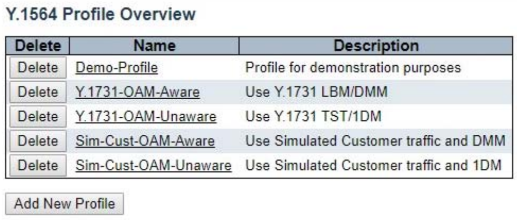
Y.1564 Test Profile

A Y.1564 profile describes parameters for the individual tests to perform along with general parameters such as test traffic type and SAC. Profiles are saved to running-config and may be re-used to perform Y.1564 tests on any EVC.

To manage the saved Y.1564 test profiles listed on the Y.1564 **Profiles Overview** page, perform the following steps:

1. Click **Configuration** > **Traffic Test** > **Y.1564** > **Profiles**, and click the specific profile name to view all the configurations of any existing test profile.

Figure 3 • **Y.1564 Profile Overview Web Page**



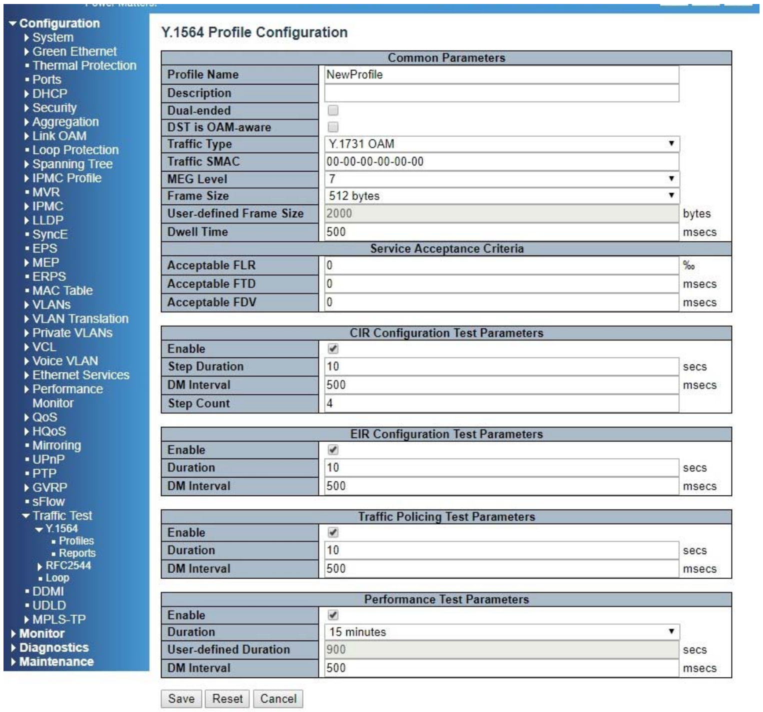
Y.1564 Profile Overview

Delete	Name	Description
Delete	Demo-Profile	Profile for demonstration purposes
Delete	Y.1731-OAM-Aware	Use Y.1731 LBM/DMM
Delete	Y.1731-OAM-Unaware	Use Y.1731 TST/1DM
Delete	Sim-Cust-OAM-Aware	Use Simulated Customer traffic and DMM
Delete	Sim-Cust-OAM-Unaware	Use Simulated Customer traffic and 1DM

2. Click **Delete** to delete the profile from running-config.

3. To create a new profile, click **Add New Profile**, and on the **Profile Configuration** page set up the required parameters for the new test as shown in the following illustration.

Figure 4 • **Newly Created Profile with Default Values**



Y.1564 Profile Configuration

Common Parameters		
Profile Name	NewProfile	
Description		
Dual-ended	☐	
DST is OAM-aware	☐	
Traffic Type	Y.1731 OAM ▾	
Traffic SMAC	00-00-00-00-00-00	
MEG Level	7 ▾	
Frame Size	512 bytes ▾	
User-defined Frame Size	2000	bytes
Dwell Time	500	msecs
Service Acceptance Criteria		
Acceptable FLR	0	‰
Acceptable FTD	0	msecs
Acceptable FDV	0	msecs

CIR Configuration Test Parameters		
Enable	☑	
Step Duration	10	secs
DM Interval	500	msecs
Step Count	4	

EIR Configuration Test Parameters		
Enable	☑	
Duration	10	secs
DM Interval	500	msecs

Traffic Policing Test Parameters		
Enable	☑	
Duration	10	secs
DM Interval	500	msecs

Performance Test Parameters		
Enable	☑	
Duration	15 minutes ▾	
User-defined Duration	900	secs
DM Interval	500	msecs

4. Click **Save** to return to the profile overview page, where the new profile will be listed in the table of all profiles. There can be up to 16 different profiles.

   Test profiles can also be shown using the following ICLI command.

```
# show y1564 profile

Profile Name                        Description
--------------------------------    --------------------------------
Demo-Profile                        Profile for demonstration purposes
Y.1731-OAM-Aware                    Use Y.1731 LBM/DMM
Y.1731-OAM-Unaware                  Use Y.1731 TST/1DM
Sim-Cust-OAM-Aware                  Use Simulated Customer traffic and DMM
Sim-Cust-OAM-Unaware                Use Simulated Customer traffic and 1DM
```

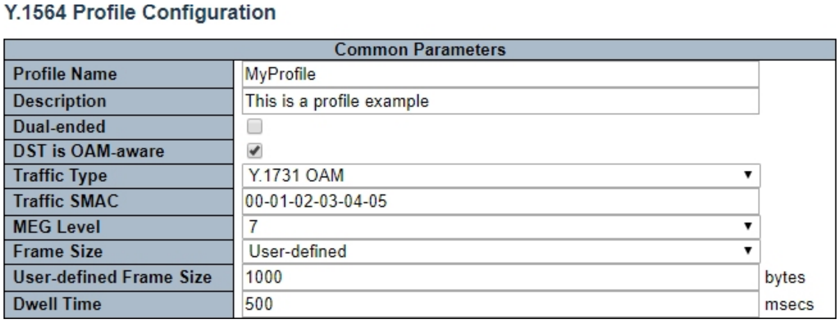
To create a new Y.1564 profile or rename an existing profile through ICLI, the user needs to enter configuration mode. See the following example to create a new Y.1564 profile, `MyProfile`:

```
! Get into configuration mode
# configure terminal
! Create a Y.1564 test profile and name it "MyProfile".
! If a profile named "MyProfile" already exists, the command that follows will
! modify the existing profile instead of creating a new profile.
(config)# y1564 profile MyProfile
(configure-y1564-profile)#
```

Common Parameters

In the profile configuration web page, all the common parameters and sub-test specific parameters in a test profile are shown graphically. The configuration is straight forward.

Figure 5 • **Common Parameters**



Y.1564 Profile Configuration

Common Parameters		
Profile Name	MyProfile	
Description	This is a profile example	
Dual-ended	□	
DST is OAM-aware	☑	
Traffic Type	Y.1731 OAM ▾	
Traffic SMAC	00-01-02-03-04-05	
MEG Level	7 ▾	
Frame Size	User-defined ▾	
User-defined Frame Size	1000	bytes
Dwell Time	500	msecs

Table 1 • **Common Parameters**

Parameters	Description
Profile Name	Each profile must have a unique name of up to 32 characters to associate with. Default: NewProfile
Description	A textual description up to 128 characters associated with the profile. Default: blank
Dual-ended	When the option is selected, the test flows are generated at SRC and statistics are gathered at DST. Test traffic only travels the network once. This is not currently supported, so leave it unchecked. If unchecked, single-ended measurements are performed, where SRC transmits traffic and expects a looped version to return to the SRC for statistics gathering. The report is generated by the Y.1564 software in this case.
DST is OAM-aware	When the option is selected, the device transmits Y.1731 LBM frames as background traffic, and expects the remote end to return Y.1731 Loopback Reply (LBR) frames. When the option is cleared, the device transmits Y.1731 1DM frames for delay measurements and expects the remote end to simply loop the frames without timestamping them. If selected and traffic type is Y.1731, the switch transmits Y.1731 LBM frames as test traffic and expects the remote end to return Y.1731 LBR frames. If cleared and traffic type is Y.1731, the switch transmits Y.1731 TST frames as test traffic and expects the remote end to simply loop the frames and return them as Y.1731 TST frames. By default the checkbox is cleared.

Table 1 • **Common Parameters (continued)**

Parameters	**Description**
Traffic Type	Drop-down box has two options: Y.**1731 OAM** and **Simulated Customer**. Defaults to Y.1731 OAM. When set to Y.**1731 OAM**, Y.1731 OAM frames are transmitted from the local end according to the description of DST is OAM-aware. When set to **Simulated Customer Traffic**, the Y.1564 software generates a traffic-pattern that is supposed to match the ECE. This provides the best option for testing that no other ECEs accidentally capture the applied UNI ingress traffic. The remote end may be a simple EVC MAC-loop - preferably at UNI to test the whole UNI-to-UNI path.
Traffic SMAC	The source MAC (SMAC) address used in the background traffic frames regardless of the setting of the **Traffic Type** parameter. If used the address must be a non-zero, unicast address. The default value for this parameter is all-zeros. In this case the value is not used and the MEP native MAC address is used instead. This parameter only applies to the generated background traffic. DM OAM frames always uses the UNI port's native MAC address as their SMAC address.
MEG Level	Specifies the MEG level in all Y.1731 OAM frames (LBM/TST/DMM/1DM) that may be generated by the SRC switch.
Frame Size	Controls the frame size of the test traffic (not the DM traffic). Specifies the frame sizes for each test. select from: 64, 128, 256, 512, 1024, 1280, 1518, MTU, and User-defined. Default:512 bytes. If MTU is selected, the Y.1564 software finds the UNI port's MTU during test execution and generates frames including various UNI ingress VLAN tags that amounts to the MTU. Notice that if an additional (S-) tag is applied on NNI, the MTU of NNI must be four bytes bigger than the MTU of UNI.
User-defined Frame Size	If Frame Size is set to User-defined, this one controls the frame size used in the test traffic. Default: 2000 btyes.
Dwell time	Specifies the number of milliseconds to wait after each trial for the test to settle before reading statistics from the hardware. Default: 500 milliseconds

The above common parameters for a Y.1564 test profile can also be configured through the ICLI interface. Below is an example of configuring the common parameters for test profile, `MyProfile`.

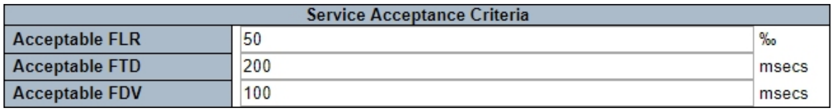
```
! Create a Y.1564 profile named "MyProfile"
(config)# y1564 profile MyProfile
! Add a description to the profile
```

```
(config-y1564-profile)# description This is a profile example
! Set destination to be OAM-aware so that Y.1731 LBM and DMM frames will be used
! rather than Y.1731 TST and 1DM frames.
(config-y1564-profile)# dst-oam-aware
! Set traffic type to 'oam' to use Y.1731 OAM frames for test traffic.
! Alternative is 'customer-simulated'.
(config-y1564-profile)# traffic-type oam
! Choose a particular Source MAC address to be used in the generated frames
! Notice that this is not available in all products.
(config-y1564-profile)# traffic-smac 00-01-02-03-04-05
! Set MEG level
(config-y1564-profile)# meg-level 7
! The EMIX-abbreviations outlined in the ITU-T Y.1564 Recommendation is used.
! The Y.1564 software only supports an EMIX-length of 1.
! Set the frame size to a user-defined size (EXMI letter = 'u')
(config-y1564-profile) # emix u
! Set the user-defined frame size to 1000 bytes.
(config-y1564-profile)# user-defined-frame-size 1000
! set dwell time to be 500 ms
(config-y1564-profile)# dwell-time 500
```

Service Acceptance Criteria (SAC)

SAC is a set of parameters used to ensure that the service meets its functionality and quality requirements and that the service provider is ready to operate the new service when it has been deployed. The SAC is also use as the PASS criteria for each of the Y.1564 sub-tests.

Figure 6 • **Service Acceptance Criteria**



Service Acceptance Criteria		
Acceptable FLR	50	‰
Acceptable FTD	200	msecs
Acceptable FDV	100	msecs

Table 2 • **Service Acceptance Criteria**

Criteria	Description
Acceptable FLR	The maximum acceptable frame loss rate in the range [1; 1000]%. Let the number of In-Service UNI Ingress frames be Tx and the number of UNI Egress frames be Rx. The frame loss ratio in ‰ is defined as 1000 * (Tx - Rx) / Tx. The In-Service UNI Ingress frame count is the number of frames that actually pass through the policer. FLR-checks are only performed on green flows, as yellow frames may get dropped along the way from SRC to DST (and reverse). FLR-checks are performed on both test traffic and DM traffic.

Table 2 • **Service Acceptance Criteria (continued)**

Criteria	Description
Acceptable FTD	Specifies the maximum frame transfer delay in milliseconds. A value of 0 (default), disables the check. The FTD-check is made on Y.1731 DMM/DMR and 1DM frames. These frames are always 64 or 68 bytes independent of the profile's Frame Size. The frames are transmitted by software, timestamped by hardware and analyzed by software upon reception, and they always bypass the policer on UNI ingress. This value is only used if transmission of DM frames is enabled.
Acceptable FDV	Specifies the maximum allowed delay variation in milliseconds. A value of 0 (default), disables the check. The FDV-check is made on Y.1731 DMM/DMR and 1DM frames. This value is only used if the transmission of DM frames is enabled.

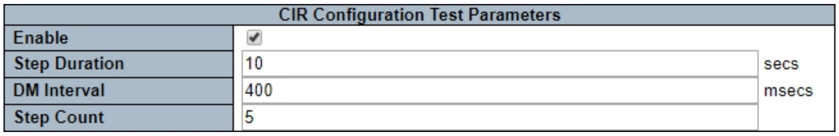
The SAC parameters can be entered in the web GUI as shown in Figure 6, page 16 or through ICLI using the following commands.

```
! Set acceptable frame loss ratio to be 50 permille
(config-y1564-profile)# acceptable-flr 50
!Set acceptable frame transfer delay to be 200 ms
(config-y1564-profile)# acceptable-ftd 200
! Set acceptable frame delay variation to be 100 ms
(config-y1564-profile)# acceptable-fdv 100
```

CIR Configuration Test

The CIR configuration test is carried out as outlined in CIR Configuration Test, page 21-10. This section discusses the CIR configuration test parameters.

Figure 7 • **CIR Configuration Test Configuration**



CIR Configuration Test Parameters		
Enable	☑	
Step Duration	10	secs
DM Interval	400	msecs
Step Count	5	

Table 3 • **CIR Configuration Test Parameters**

Test Parameters	Description
Enable	Select the option to enable the execution of CIR configuration test. Default: Selected.
Step Duration	Specifies the number of seconds each step runs. Default: 10 seconds

Table 3 • **CIR Configuration Test Parameters (continued)**

Test Parameters	Description
DM Interval	Specifies the number of milliseconds between transmission of each DM frame into UNI ingress. Default: 500 milliseconds Delay measurements can be disabled for this test by specifying a value of 0.
Step Count	Specifies the number of steps for step load CIR test. Default: 4. A value of 1 will apply 100% CIR in one go. If the CIR of policer divided by the step count is less than 1 Mbps, then the test does not start.

The following is an example to enable a CIR test, set DM interval to 400 ms, set step duration to 10 seconds, and with 5 steps (so that traffic rates of 20%, 40%, 60%, 80%, 100% * CIR will be tested).

```
(config-y1564-profile)# cir-test dm-interval 400 duration 10 step-count 5
```

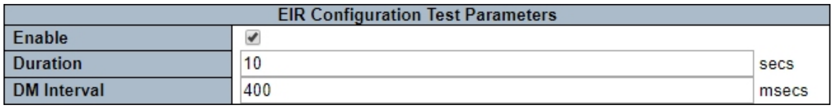
This snippet disables the CIR configuration test:

```
(config-y1564-profile)# no cir-test
```

EIR Configuration Test

The EIR configuration test is carried out as outlined in EIR Configuration Test. This section discusses the EIR configuration test parameters.

Figure 8 • **EIR Configuration Test Configuration**



EIR Configuration Test Parameters

Enable	☑	
Duration	10	secs
DM Interval	400	msecs

Table 4 • **EIR Configuration Test Parameters**

Test Parameters	Description
Enable	Select the option to enable execution of the EIR configuration test. Default: Selected
Duration	Specifies the number of seconds the test runs. Default: 10 seconds
DM Interval	Specifies the number of milliseconds between transmission of each DM frame into UNI ingress. Default: 500 milliseconds Delay measurements can be disabled for this test by specifying a value of 0.

The following is an example to enable EIR test, set DM interval to 400 ms, set test duration to 10 seconds.

```
(config-y1564-profile)# eir-test duration 10 dm-interval 400
```

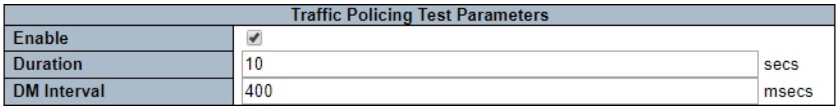
This snippet disables the EIR configuration test:

```
(config-y1564-profile)# no eir-test
```

Traffic Policing Test

The traffic policing test is carried out as outlined in Traffic Policing Test, page 21-11. This section discusses the traffic policing test parameters.

Figure 9 • **Traffic Policing Test Configuration**



Traffic Policing Test Parameters		
Enable	☑	
Duration	10	secs
DM Interval	400	msecs

Table 5 • **Traffic Policing Test Parameters**

Test Parameters	Description
Enable	Select the option to enable the execution of the traffic policing test. Default: Selected
Duration	Specifies the number of seconds the test will run. Default: 10 seconds
DM Interval	Specifies the number of milliseconds between transmission of each DM frame into UNI ingress. Default: 500 milliseconds Delay measurements can be disabled for this test by specifying a value of 0.

The following is an example to enable traffic policing test, set DM interval to be 400 ms, set step duration to be 10 seconds.

```
(config-y1564-profile)# traffic-policing-test duration 10 dm-interval 400
```

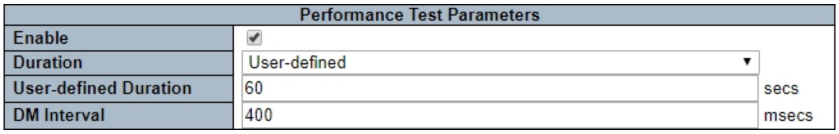
This snippet disables the traffic policing test:

```
(config-y1564-profile)# no traffic-policing-test
```

Service Performance Test

The service performance test (also simply known as "performance test") is carried out as outlined in Service Performance Test, page 21-12. This section discusses the performance test parameters.

Figure 10 • **Performance Test Configuration**



Performance Test Parameters		
Enable	☑	
Duration	User-defined ▾	
User-defined Duration	60	secs
DM Interval	400	msecs

Table 6 • **Performance Test Parameters**

Test Parameters	Description
Enable	Select the option to enable execution of the performance test. Default: Selected
Duration	Specifies the number of seconds the performance test runs. Supported duration are: 15 minutes, 2 hours, 24 hours, and user-defined (which allows for a custom duration specified in user-defined duration below). Default: 15 minutes

Table 6 • **Performance Test Parameters (continued)**

Test Parameters	Description
User-defined Duration	If Duration is set to User-defined, this one chooses the actual duration of the test, measured in seconds. Default: 900 seconds
DM Interval	Specifies the number of milliseconds between transmission of each DM frame into UNI ingress. Default: 500 milliseconds

The following is an example to enable traffic policing test, set DM interval to 400 ms, and set the step duration to 60 seconds. And finish configuration of the profile.

```
(config-y1564-profile)# performance-test duration 60 dm-interval 400
```

This snippet disables the traffic policing test:

```
(config-y1564-profile)# no performance-test
```

The configured Y.1564 test profile can be shown using the following show command followed by the profile name:

```
# show y1564 profile MyProfile

Profile configuration:
  Profile name                : MyProfile
  Description                 : This is a profile example
  Measurement type            : Single-ended (DST loops traffic)
  DST is OAM aware            : Yes
  Test traffic type           : Y.1731 LBM
  Test traffic SMAC           : 00-01-02-03-04-05
  Delay measurement type      : Y.1731 DMM
  MEG Level                   : 7
  Dwell time                  : 500 msecs
  Frame size                  : User-defined (EMIX=u)
  User-defined frame size     : 1000 bytes
  CIR configuration test      : Enabled
  EIR configuration test      : Enabled
  Traffic policing test       : Enabled
  Service performance test    : Enabled
  Acceptable FLR              : 50 permille
  Acceptable FTD              : 200 msecs
  Acceptable FDV              : 100 msecs

CIR configuration test configuration:
  Duration per step           : 10 seconds
  Delay meas. interval        : 400 msecs
  Step count                  : 4

EIR configuration test configuration:
  Duration                    : 10 seconds
  Delay meas. interval        : 400 msecs

Traffic policing test configuration:
  Duration                    : 10 seconds
  Delay meas. interval        : 400 msecs

Service performance test configuration:
  Duration                    : 60 seconds
  Delay meas. interval        : 400 msecs
```

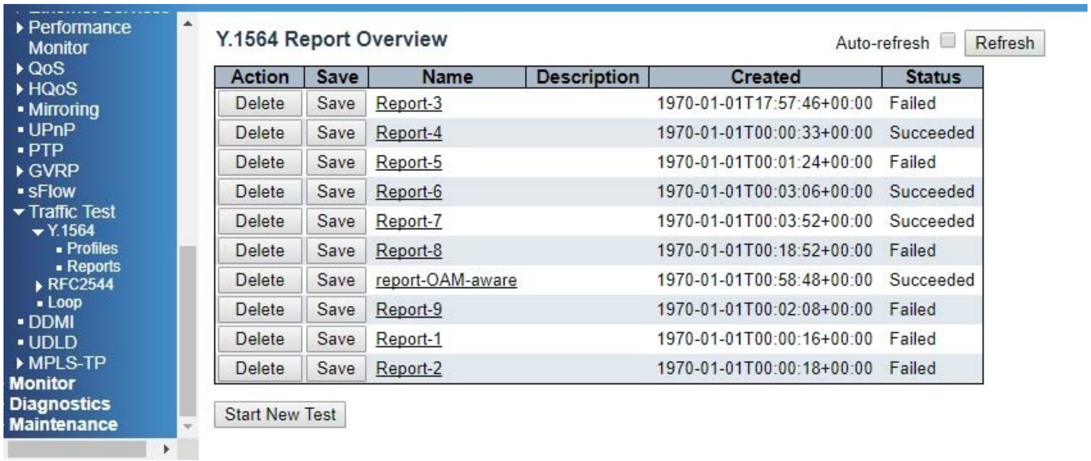
Y.1564 Test and Report

A new Y.1564 test report is automatically generated and saved after each Y.1564 test is executed.

To manage the test reports, perform the following steps.

1. Click **Configuration** > **Traffic Test** > **Y.1564** > **Reports**, the **Y.1564 Report Overview** page opens. The contents of any test report can be viewed by clicking the report name.
2. To delete a test report, click **Delete**.
3. To download a test report and save it as a TXT file, Click **Save** of any test report.

Figure 11 • **Y.1564 Report Overview Page**



Y.1564 Report Overview

Action	Save	Name	Description	Created	Status
Delete	Save	Report-3		1970-01-01T17:57:46+00:00	Failed
Delete	Save	Report-4		1970-01-01T00:00:33+00:00	Succeeded
Delete	Save	Report-5		1970-01-01T00:01:24+00:00	Failed
Delete	Save	Report-6		1970-01-01T00:03:06+00:00	Succeeded
Delete	Save	Report-7		1970-01-01T00:03:52+00:00	Succeeded
Delete	Save	Report-8		1970-01-01T00:18:52+00:00	Failed
Delete	Save	report-OAM-aware		1970-01-01T00:58:48+00:00	Succeeded
Delete	Save	Report-9		1970-01-01T00:02:08+00:00	Failed
Delete	Save	Report-1		1970-01-01T00:00:16+00:00	Failed
Delete	Save	Report-2		1970-01-01T00:00:18+00:00	Failed

The existing test reports can also be shown with the following ICLI commands:

```
# show y1564 report
Report Name                       Created                     Status
--------------------------------  -------------------------   -----------------
Report-3                          1970-01-01T17:57:46+00:00   Failed
Report-4                          1970-01-01T00:00:33+00:00   Succeeded
Report-5                          1970-01-01T00:01:24+00:00   Failed
Report-6                          1970-01-01T00:03:06+00:00   Succeeded
Report-7                          1970-01-01T00:03:52+00:00   Succeeded
Report-8                          1970-01-01T00:18:52+00:00   Failed
report-OAM-aware                  1970-01-01T00:58:48+00:00   Succeeded
Report-9                          1970-01-01T00:02:08+00:00   Failed
Report-1                          1970-01-01T00:00:16+00:00   Failed
Report-2                          1970-01-01T00:00:18+00:00   Failed
```

Note Reports are shown in ascending chronological order (newest last).

A test report can be downloaded with the following ICLI commands:

`y1564 save <report-name> <url>,`
where `<url>` is on the following form:

```
    tftp://[<username>[:<password>]@]<host>[:<port>][/<path>]
```

y1564 save <report-name> <url>, where <url> is on the following form:

tftp://[<username>[:<password>]@]<host>[:<port>][/<path>]

The corresponding CLI command to delete a test report is:

```
y1564 delete <report-name>
```

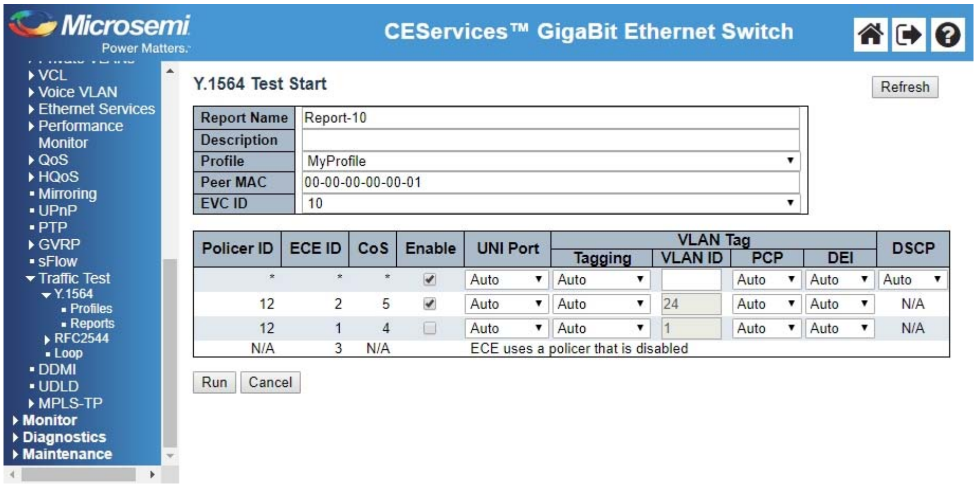
The contents of any test report can be viewed by appending the report name to the above command.

Starting a Y.1564 Test

To start a Y.1564 test, perform the following step.

- On the **Y.1564 Report Overview** page, click **Start New Test** to view the result as shown in the following illustration.

Figure 12 • **Example of Starting a Y.1564 Test**



Y.1564 Test Start

Report Name	Report-10
Description	
Profile	MyProfile ▾
Peer MAC	00-00-00-00-00-01
EVC ID	10 ▾

Policer ID	ECE ID	CoS	Enable	UNI Port	VLAN Tag				DSCP
					Tagging	VLAN ID	PCP	DEI	
*	*	*	☑	Auto ▾	Auto ▾		Auto ▾	Auto ▾	Auto ▾
12	2	5	☑	Auto ▾	Auto ▾	24	Auto ▾	Auto ▾	N/A
12	1	4	☐	Auto ▾	Auto ▾	1	Auto ▾	Auto ▾	N/A
N/A	3	N/A		ECE uses a policer that is disabled					

The following table describes all the parameters in the web interface.

Table 7 • **Y.1564 Test Start Parameters**

Test Parameters	Description
Report Name	Specifies a name of the resulting report. The name may be from 1 to 32 ASCII characters long (some special characters are not allowed). If none specified, the Y.1564 software auto-picks one.
Description	An optional description of the report of 0 to 128 characters. Default: Blank.
Profile	Drop-down box with all the known Y.1564 profiles (see Y.1564 Test Profile. Default: First saved profile The selected profile will be used when executing the test.
Peer MAC	The MAC address used as destination MAC in the generated test and DM traffic. Default: 00-00-00-00-00-01 When the profile's **DST is OAM-aware** option is selected, the peer MAC must be specified correctly. It is the MAC address of the switch port on which the OAM-loop is created. See Y.1564 Test Type vs. Traffic Test Loop Type for a description of finding the Peer MAC on a Cisco switch.

Table 7 • **Y.1564 Test Start Parameters (continued)**

Test Parameters	Description
EVC ID	Drop-down box with all the created EVCs. Default: The lowest numbered EVC ID This is the EVC on which the Y.1564 test will be executed. Changing the EVC ID also changes the table, which holds a list of all the ECEs specified on that EVC. One or more ECEs may map to a single EVC with different CoS and bandwidth profiles (policers). For an EVC and ECE configuration guide, please refer to ENT-AN1037 application note.
Policer ID	Specifies the policer ID of the ECE. The whole table is first sorted by policer ID, then by ECE ID in hardware-order. The reason it is sorted by policer ID is that only one ECE out of several that maps to the same policer can be tested at a time. If the ECE does not have a policer associated with it or if the policer is disabled, the ECE will not be testable, and the row will contain an explanation. In the previous illustration, ECE #3 is not testable, because the policer it uses is disabled. When this is the case, it is not possible to include it in the tested ECEs, but the test can be started for other testable ECEs.
ECE ID	Specifies the ID of the ECE. If all ECEs map to different policers, the ECEs are shown in the same order as they appear in hardware.
CoS	Specifies the CoS the ECE maps to. On the ECE configuration page, this corresponds to the **Class** field. of the **Action** table. For an ECE to be testable, it must map to a particular CoS.
Enable	Select the ECEs to perform a Y.1564 test on. Up to 8 ECEs can be tested simultaneously. By default, all testable ECEs are selected. If more than one ECE uses the same policer, only one of these can be checked at a time. The Y.1564 software automatically clears other ECEs that map to the same policer as the one that gets selected.
UNI Port	A drop-down list with all the UNI ports of ECEs available. Default is **Auto** that means that the Y.1564 software automatically picks a UNI from the possible list of UNIs for that ECE. When the profile uses Y.1731 as test traffic, all ECEs selected for test must use the same UNI port.
Tagging	Drop-down list with the tagging options for the ECE in question. The drop-down list always contains the **Auto** option, which means that it is up to the Y.1564 software to pick a suitable tag-type and VLAN ID when testing the ECE. The two other possible values are: **Untagged** and **Specific**. If the ECE matches untagged traffic, **Untagged** is available. If the ECE matches VLAN tagged traffic **Specific** is available in the drop-down list.
VLAN ID	This is only available if **Tagging** is set to **Specific**. It allows the user to select a particular VLAN ID to be used in the generated packets for that ECE. The test does not start, if the selected VLAN ID is not within the matching range of ECE.
PCP	Specifies the PCP value used in the VLAN tag (if present) of the UNI ingress traffic for this ECE. Default is **Auto** that means that the Y.1564 software selects a suitable PCP value itself. This value is only used if the **Traffic Type** of the selected profile is set to **Simulated Customer**. For Y.1731 test traffic, the PCP value will be that of the CoS the ECE maps to.

Table 7 • **Y.1564 Test Start Parameters (continued)**

Test Parameters	Description
DEI	Specifies the DEI value used in the VLAN tag (if present) of the UNI ingress traffic for this ECE. The DEI value normally controls the color of the ingress traffic through classification of DEI to Drop Precedence (DP), but several things may cause the DP not to follow the DEI. The ECE, for instance, may force all the traffic into a particular DP, making the DEI irrelevant, or the UNI's QoS Ingress Port Tag Classification configuration may cause a DEI of 0 to map to a DP of 1. If set to **Auto** (which is the default), the Y.1564 software analyzes the color a flow with DEI 0 will have when it reaches the policer, and the color a flow with DEI 1 will have when it reaches the policer. If both DEI values result in the same color, only one flow is generated, otherwise two flows are generated when needed. The drop-down list has two other values: **0** and **1**. Selecting either causes at most one flow to be generated. The Y.1564 software analyzes the color of that flow when it reaches the policer. So, typically one can restrict the test to green-only flows or yellow-only flows by selecting a value different from **Auto**.
DSCP	Specifies the DSCP used if the ECE matches IP frames. **Auto** causes the Y.1564 software to pick one from the valid range of DSCP values. It is only used when **Traffic Type** of profile is **Simulated Customer**.

Y.1564 Test Execution

Once the ECEs of EVC and the associated parameters are selected, click **Run** to start test. The corresponding CLI command syntax is:

```
y1564 start <report-name> profile <profile-name> evc <evc-id> [peer-mac
<peer-mac-address>] {[ece <ece-id> [interface <uni>] [vlan <vlan-id> | priority-tagged |
untagged] [pcp <0-7>] [dei <0-1>] [dscp [0-63]) * 8]} {[desc <description>]}
```

Basically, it says: Start a Y.1564 test on EVC #`<evc-id>` using the profile called `<profile-name>`. Save the result in `<report-name>`. Optionally, provide a Peer MAC address as `<peer-mac-address>` and choose up to 8 individual ECEs to test. For each ECE, optionally choose the UNI, the VLAN ID, PCP, DEI, and DSCP to use, and end the command with an optional description. If no ECEs are specified, the Y.1564 software picks all the ECEs defined for the EVC in question. Leaving out any of the optional ECE parameters corresponds to choosing **Auto** in the web interface.

Assuming the user has fixed the missing enabling of policer of ECE #3 from Figure 12, page 22, the test can be started with the following CLI command:

```
# y1564 start Report-10 profile MyProfile evc 10 peer-mac 00-01-c1-00-b5-33 ece 2 ece 3
```

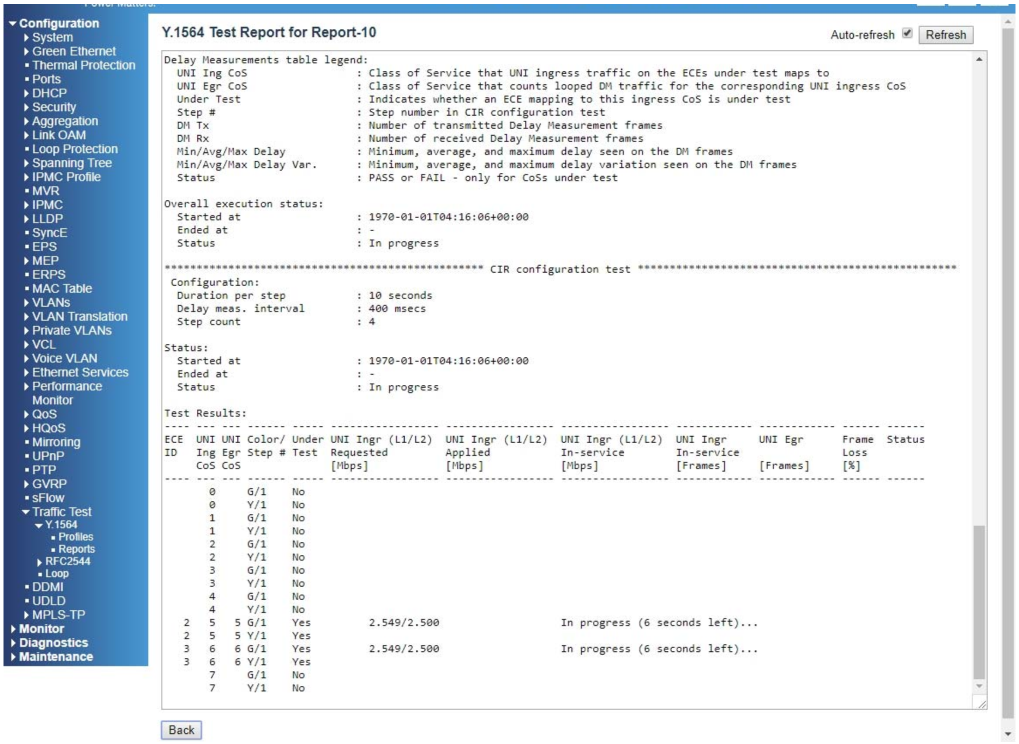
Notice, only one test can be in progress at a time.

At this stage, a number of checks will be done before the actual test traffic gets applied. If either of these checks fails, the Y.1564 software will refuse to start the test and print an appropriate error message. No report will be saved in that case.

The checks depend on many things, for instance, the chosen profile's Traffic Type and the chosen UNIs and DEI values.

Once the test has passed all the leading checks, the actual test execution will begin. If started from the Web GUI, the browser redirects to the Y.1564 Test Report Web page, showing live status and statistics as long as the test executes. Once the test completes, the live-update (**Auto-refresh** checkbox) disables itself. If started from CLI, nothing else is displayed, but the user may request the current status by using the `show y1564 report` command or show the live report by appending the report name to that CLI command.

Figure 13 • **Example of Test Report While Executing**



Y.1564 Test Report for Report-10

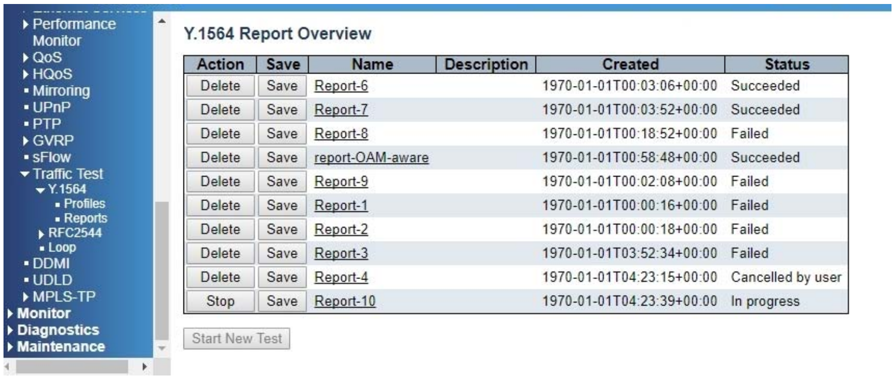
```
Delay Measurements table legend:
  UNI Ing CoS               : Class of Service that UNI ingress traffic on the ECEs under test maps to
  UNI Egr CoS               : Class of Service that counts looped DM traffic for the corresponding UNI ingress CoS
  Under Test                : Indicates whether an ECE mapping to this ingress CoS is under test
  Step #                    : Step number in CIR configuration test
  DM Tx                     : Number of transmitted Delay Measurement frames
  DM Rx                     : Number of received Delay Measurement frames
  Min/Avg/Max Delay         : Minimum, average, and maximum delay seen on the DM frames
  Min/Avg/Max Delay Var.    : Minimum, average, and maximum delay variation seen on the DM frames
  Status                    : PASS or FAIL - only for CoSs under test

Overall execution status:
  Started at                : 1970-01-01T04:16:06+00:00
  Ended at                  : -
  Status                    : In progress

************************************************** CIR configuration test **************************************************
 Configuration:
  Duration per step         : 10 seconds
  Delay meas. interval      : 400 msecs
  Step count                : 4

Status:
  Started at                : 1970-01-01T04:16:06+00:00
  Ended at                  : -
  Status                    : In progress

Test Results:
---- --- --- ------ ----- ---------------- ---------------- ---------------- ----------- ----------- ------ ------
ECE  UNI UNI Color/ Under UNI Ingr (L1/L2) UNI Ingr (L1/L2) UNI Ingr (L1/L2) UNI Ingr    UNI Egr     Frame  Status
ID   Ing Egr Step # Test  Requested        Applied          In-service       In-service              Loss
     CoS CoS              [Mbps]           [Mbps]           [Mbps]           [Frames]    [Frames]    [%]
---- --- --- ------ ----- ---------------- ---------------- ---------------- ----------- ----------- ------ ------
       0    G/1    No
       0    Y/1    No
       1    G/1    No
       1    Y/1    No
       2    G/1    No
       2    Y/1    No
       3    G/1    No
       3    Y/1    No
       4    G/1    No
       4    Y/1    No
   2   5   5 G/1    Yes        2.549/2.500                      In progress (6 seconds left)...
   2   5   5 Y/1    Yes
   3   6   6 G/1    Yes        2.549/2.500                      In progress (6 seconds left)...
   3   6   6 Y/1    Yes
       7    G/1    No
       7    Y/1    No
```

The status of the test will be `In progress` as long as it has not completed. The test may be aborted with `y1564 stop <report-name>`, like this:

```
# y1564 stop Report-10
```

Or click the **Stop** button on the **Report Overview** page (press the **Back** in the previous illustration). Doing so will cause the Status to change to Canceled by user.

Figure 14 • **Aborting a Test in progress**



Y.1564 Report Overview

Action	Save	Name	Description	Created	Status
Delete	Save	Report-6		1970-01-01T00:03:06+00:00	Succeeded
Delete	Save	Report-7		1970-01-01T00:03:52+00:00	Succeeded
Delete	Save	Report-8		1970-01-01T00:18:52+00:00	Failed
Delete	Save	report-OAM-aware		1970-01-01T00:58:48+00:00	Succeeded
Delete	Save	Report-9		1970-01-01T00:02:08+00:00	Failed
Delete	Save	Report-1		1970-01-01T00:00:16+00:00	Failed
Delete	Save	Report-2		1970-01-01T00:00:18+00:00	Failed
Delete	Save	Report-3		1970-01-01T03:52:34+00:00	Failed
Delete	Save	Report-4		1970-01-01T04:23:15+00:00	Cancelled by user
Stop	Save	Report-10		1970-01-01T04:23:39+00:00	In progress

Test execution will stop by itself as soon as one test fails or when all the enabled tests pass. The **Status** in these cases will be **Failed** and **Succeeded**, respectively.

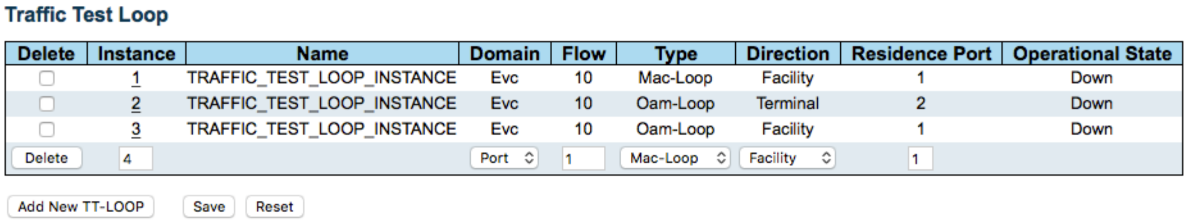
Traffic Test Loop Configuration

Since the dual-ended testing is not supported with the current version of the Y.1564 software, the remote end must be configured to loop frames. In order to do so, use the traffic test loop functionality described in details in ENT-AN1230 application note. In the following, a brief overview is given.

A test loop is installed on the DST switch to match frames it receives at certain point inside the switch with the configured parameter and sends the frames back so that the Y.1564 SRC can gather statistics for the test. To configure a TT-LOOP (Traffic Test Loop) on the web interface, perform the following steps:

1. Click **Configuration** > **Traffic Test** > **Loop**. The **Traffic Test Loop** page opens as shown in the following illustration.

Figure 15 • **Add New Traffic Test Loop**



Traffic Test Loop

Delete	Instance	Name	Domain	Flow	Type	Direction	Residence Port	Operational State
□	1	TRAFFIC_TEST_LOOP_INSTANCE	Evc	10	Mac-Loop	Facility	1	Down
□	2	TRAFFIC_TEST_LOOP_INSTANCE	Evc	10	Oam-Loop	Terminal	2	Down
□	3	TRAFFIC_TEST_LOOP_INSTANCE	Evc	10	Oam-Loop	Facility	1	Down
Delete	4		Port	1	Mac-Loop	Facility	1	

2. To create and configure a new Traffic Test Loop, click **Add New TT-LOOP** and configure the following parameters:

Table 8 • **Traffic Test Loop Parameters**

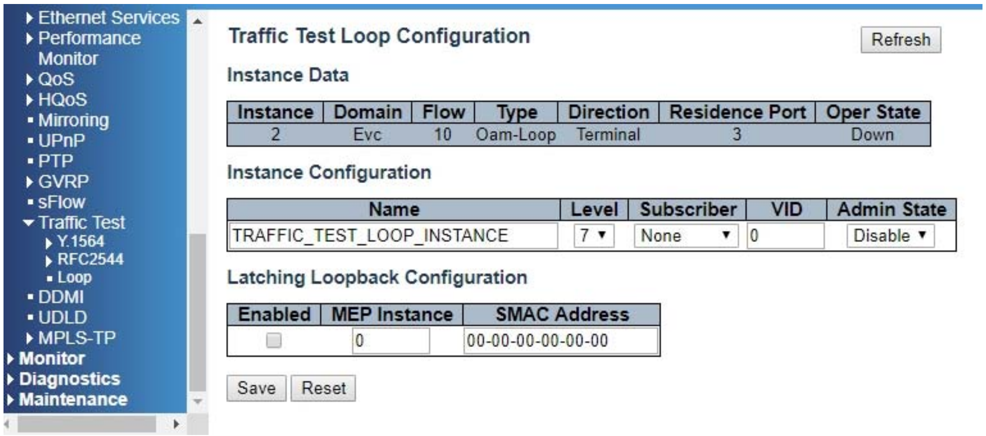
Parameters	Description
Delete	Select to delete the loop instance when **Save** button is clicked.
Instance ID	The ID of the new TT-LOOP. Once a TT-LOOP is created the parameters of that TT-LOOP can be modified by clicking the ID.
Name	A symbolic name for the loop. If not specified, the Traffic Test Loop software picks one by itself. Loop name modification is shown later.
Domain	Specifies the domain of the loop. Possible values are **Port**, **EVC**, and, **VLAN**. Flow is a sub-parameter to the domain, as follows: • **Port**: All frames received on the residence port are looped. **Flow** is not used. • **EVC**: All frames on a given EVC are looped. The EVC must be created before configuring the loop. **Flow** is the EVC ID. • **VLAN**: Loop all frames received on a given VLAN. **Flow** is the VLAN ID.

Table 8 • **Traffic Test Loop Parameters (continued)**

Parameters	Description
Type	Selects either **mac_loop** or **oam-loop**. A mac-loop matches all frames belongs to the configured domain and swaps the **SMAC** and **DMAC** and clears the multicast bit of the resulting SMAC before looping them back. An oam_loop is actually an MEP that matches and responds to OAM frames intended for it. **Peer-mac** and **MEG-level** must be configured correctly for an oam-loop to work. The oam-loop responds to a Y.1731 LBM frame with a Y.1731 LBR frame and to Y.1731 DMM frame with a Delay Measurement Reply (DMR) frame.
Direction	Drop-down list with two options: **Facility** and **Terminal**. A **facility loop** loops from ingress to egress, that is, frames that ingress the residence port and are subject to looping are looped back out on the residence port. A **terminal loop** loops from egress to ingress, that is, frames that are supposed to egress the residence port and are subject to looping are looped back to the ingress port.
Operational State	They can be **Down** or **Up**. If **Down**, the loop is not active, either because it is not administratively enabled or because not all the resources are available. If **Up**, all the resources are available and allocated and the loop is administratively enabled. Administrative state modification is discussed later.
OpState Control	Indicates the mechanism for controlling the operational state of the loop. Change of the operational state control is shown later. It takes two values: • **Static**: The loop is controlled by management commands, that is, the operational state is fully controlled by the administrative state. • **Latch. LB**: The loop is controlled by the MEF 46 Latching Loopback (LL) protocol. The administrative state can control whether the loop responds to LL PDUs but the loop only enters the active state upon reception of a valid LLM activate PDU from a remote host. **Note:** This feature is not available in all products.

After a TT-LOOP instance is created and saved its operational status will still be **Down**, until it is administratively enabled. In the web interface, click the loop instance ID, which takes you to the **Traffic Test Loop Configuration** page where you can enable the loop instance as shown in the following illustration.

Figure 16 • **Configuring of Particular Loop Instance**



Traffic Test Loop Configuration

Instance Data

Instance	Domain	Flow	Type	Direction	Residence Port	Oper State
2	Evc	10	Oam-Loop	Terminal	3	Down

Instance Configuration

Name	Level	Subscriber	VID	Admin State
TRAFFIC_TEST_LOOP_INSTANCE	7 ▾	None ▾	0	Disable ▾

Latching Loopback Configuration

Enabled	MEP Instance	SMAC Address
□	0	00-00-00-00-00-00

The following table describes all the parameters in the web interface.

Table 9 • **Traffic Test Loop Configuration Parameters**

Test Parameters	Description
Name	Specifies a name for the loop instance.
Level	Selects the MEG-level the loop responds to. Only available when loop **Type** is **Oam-Loop**.
Subscriber	Only available if **Domain** is **EVC**. Controls whether the loop reacts on OAM behind a possible subscriber tag (C-tag). The following assumes that the NNI tag is an S-tag and the subscriber tag is a C-tag. It takes one of the following values: • **None**: The EVC-loop instance operates purely in the main EVC domain and matches on the S-tag of EVC (if any) followed by the Y.1731 Ethertype. • **All**: The EVC-loop operates in the EVC subscriber sub-domain and matches on the S-tag of EVC (if any) followed by a possible subscriber C-tag followed by the Y.1731 Ethertype. • **VID**: The EVC-loop operates in the EVC subscriber sub-domain and matches on the S-tag of EVC (if any) followed by a C-tag with a particular VLAN ID followed by the Y.1731 Ethertype. The VID field allows to specify this VLAN ID. This is feature is not available on all products. • **Untagged**: Deprecated. Similar to None. Not available on all products. • **Test**: Deprecated. Similar to All. Not available on all products.
Admin State	Controls whether the loop is active (Enable) or inactive (Disable).
Latching Loopback Configuration	Not available on all products. Please refer to ENT-AN1230 application note for a complete description of this functionality.

The traffic loop depicted in the previous illustration can also be created through following CLI commands:

```
(config)# traffic-test-loop 2 type oam-loop level 7 interface
GigabitEthernet 1/3 direction terminal domain evc 10 admin-state
disabled
```

Y.1564 Test Type vs. Traffic Test Loop Type

In this section, we present the loop-types that may be used with a given Y.1564 profile selection.

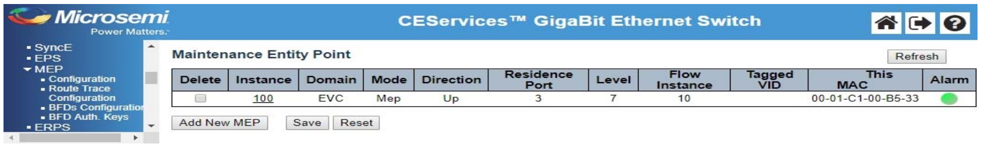
First, let us summarize:

- A **MAC-loop** is OAM unaware. It just loops back all received frames and swaps the DMAC and SMAC and clears the multicast bit of the resulting SMAC of any received frame. Peer MAC address and MEG level are irrelevant to a MAC loop.
- An **OAM-loop** is different. An OAM-loop is actually a real MEP. It only responds to OAM frames that are destined to the loop, so MEG level and peer MAC address must be configured correctly. The traffic test loop software automatically creates a special MEP once an OAM-loop gets enabled.

To find the Peer MAC address, perform the following step.

- Click **Configuration** > **MEP**.

Figure 17 • **Finding the Peer-MAC**



Maintenance Entity Point

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
□	100	EVC	Mep	Up	3	7	10		00-01-C1-00-B5-33	●

In equivalent ICLI commands are:

```
# show mep detail

MEP state is :
  Inst  cLevel  cMeg  cMep  cAis  cLck cLoop cConf  cSsf  aBlk  aTsd  aTsf  Peer MEP  cLoc  cRdi cPeriod cPrio  cDeg
   100   False False False False False False False False False False False


MEP Basic Configuration is  :
  Inst  Mode  Voe  Vola  Direct                Port    Dom  Level      Format           Name          Meg id  Mep id         Vid  Flow       Eps           MAC
   100   Mep  Voe  Vola     Up    GigabitEthernet    1/3    Evc      7      ITU ICC                     ICC  000MEG0000      1     1    10         0  00  -01-C1-00-B5-33
```

The supported combinations of Y.1564 traffic types and remote end traffic test loops are summarized in the following table.

Table 10 • **Traffic Test Loop Configurations Depending on Y.1564 Profile Configuration**

Y.1564 Profile Configuration		Traffic Test Loop Configuration		
DST is OAM-Aware	**Traffic Type**	**Type**	**Domain**	**Direction**
No	Y.1731 OAM or Simulated Customer	MAC-Loop	Port	Facility
			EVC	Facility
				Terminal

Table 10 **• Traffic Test Loop Configurations Depending on Y.1564 Profile Configuration**

Y.1564 Profile Configuration		**Traffic Test Loop Configuration**		
DST is OAM-Aware	**Traffic Type**	**Type**	**Domain**	**Direction**
Yes	Y.1731 OAM	OAM-Loop	EVC	Facility
				Terminal
	Simulated Customer	DMM: OAM-Loop and Test Traffic: MAC-Loop	EVC	OAM & MAC-Loop: Facility
				OAM & MAC-Loop: Terminal
				OAM-Loop: Facility MAC-Loop: Terminal

Notice that for DST is OAM-aware and simulated customer test traffic, two loops must be created in the EVC domain, and they must both be either facility or terminal, or OAM-loop must be facility and MAC-loop must be terminal. Also notice that DM can be turned off in the profile if all enabled sub-tests have a `DM Interval` of 0. In this case there is no difference whether DST is OAM-aware is checked or not (when using simulated customer traffic).

Use of subscriber domain `All` is recommended for all terminal loops in the EVC domain.

Understanding the Y.1564 Test Report

A Y.1564 test report includes the profile configuration, EVC, ECE, Policer, and port information, as well as detailed statistics for each of the sub-tests. This chapter starts out with describing a sample configuration of both the local and remote ends, which forms the basis of the test reports discussed in subsequent section.

Example Used

The example used in this chapter is somewhat handcrafted for the purpose, and is not considered a real-world scenario. The two ends' configuration are shown in the following two sections.

In subsequent sections, we will scrutinize the report that comes out of executing a Y.1564 test using the Web GUI *without* altering any parameters before clicking the `Run` button. In some sections, it is required to re-run the test with e.g. another profile or another set of start-parameters. In such cases, it will be mentioned.

Local End (SRC)

The example used in this chapter is given by the following EVC, ECE, and Policer configuration (CLI syntax):

```
evc policer 1 enable rate -type line cir 100000 cbs 10000 eir 25000 ebs 10000
evc policer 2 enable type single cir 75000 cbs 8000 eir 10000 ebs 4000
evc policer 3 enable mode coupled cir 50000 cbs 6000 eir 10000 ebs 6000
evc policer 4 enable cir 25000 cbs 2000 eir 10000 ebs 8000
evc 10 vid 1000 ivid 1234 interface GigabitEthernet 1/2 learning policer none
evc ece 1 interface Gi 1/3 outer-tag match type c -tagged vid 24 add pcp -mode fixed dei -mode dp pcp 5 tx-lookup pcp -vid evc 10 cos 7 dpl 0
evc ece 2 interface Gi 1/3 outer-tag match type c -tagged vid 48 add pcp -mode mapped dei -mode dp tx -lookup pcp -vid evc 10 policer 2 cos 6 dpl 1
evc ece 3 interface Gi 1/3 outer-tag match type c -tagged add dei -mode dp evc 10 policer 3 pop 1 cos 5
evc ece 4 interface Gi 1/3 outer-tag match type untagged add pcp -mode fixed dei -mode dp pcp 7 tx-lookup pcp -vid evc 10 policer 4 cos 4
```

That is, we have a tagged EVC with VLAN ID 1000 (internal VLAN ID 1234) in the S-tag on NNI, which is Gi 1/2. Learning is enabled on the EVC for debugging purposes as we shall see later.

On that EVC, we have four ECEs with the properties mentioned in the following table.

***Table 11* • Properties of Four ECEs on EVC**

	Match	Action					
ECE#	**C-tag's VLAN ID**	**Tx-Lookup**	**CoS**	**Policer #**	**Tag Pop Count**	**Drop Precedence**	**Egress Outer Tag PCP Mode**
1	24	VID-PCP	7	1	0	0	Fixed (PCP value = 5)
2	48	VID-PCP	6	2	0	1	Mapped
3	Any C-tagged	VID	5	3	1	Disabled	Classified
4	Untagged	VID-PCP	4	4	0	Disabled	Fixed (PCP value = 7)

This is a mix and match of various ECE properties. Notice, that this configuration is hand-crafted, **only** to be able to show various properties the report, and may not represent a real-world scenario.

We have two ECEs that force the Drop Precedence (DP) to 0 or 1 and two ECEs that have DP disabled, meaning that the frames will get their color from ingress classification. Two of the ECEs will not have a C-tag when they reach NNI (#3 and #4) and they all map to different CoSs.

The following table provides the policer configuration.

***Table 12* • Policer Configuration**

Policer #	Policer Type	Rate Type	CIR [kbps]	CBS [kbps]	EIR [kbps]	EBS [kbps]
1	MEF/Aware	Line (L1)	100000	10000	25000	10000
2	Single Leaky Bucket	Data (L2)	75000	8000	(10000)	(4000)
3	MEP/Coupled	Data (L2)	50000	6000	10000	6000
4	MEF/Aware	Data (L2)	25000	2000	10000	8000

MEF/Aware is a Dual Leaky Bucket, Color-Aware policer. MEF/Coupled is a Dual Leaky Bucket, Color-Aware policer with the coupling flag set. The Single Leaky Bucket policer has EIR and EBS configured, but they are not used for anything. See also Appendix A for policer types and how they work.

We will use two different Y.1564 profiles - one with Traffic Type set to Simulated Customer and one with Traffic Type set to Y.1731 OAM, like this:

```
y1564 profile profile-OAM-unaware
 traffic-type customer-simulated
 traffic-smac 00-01-02-03-04-05
 emix u
 user-defined-frame-size 1000
 cir-test duration 1 dm-interval 400 step-count 2
 eir-test duration 1 dm-interval 400
 traffic-policing-test duration 1 dm-interval 400
 performance-test duration 5 dm-interval 400
```

```
!
y1564 profile profile-OAM-aware
 dst-oam-aware
 traffic-smac 00-01-02-03-04-05
 emix u
 user-defined-frame-size 1000
 cir-test duration 1 dm-interval 400 step-count 2
 eir-test duration 1 dm-interval 400
 traffic-policing-test duration 1 dm-interval 400
 performance-test duration 5 dm-interval 400
```

We have reduced the run-time for each sub-test and we use a custom-sized frame of 1000 bytes. On tagged ECEs the actual frame size applied to UNI ingress will therefore be 1004 bytes.

Remote End (DST)

The remote end is configured with the same ECEs and policers as the local end. If and only if using a terminal MAC-loop in the EVC domain, the policers must be disabled, because only then will the test traffic AND the DM traffic go through the policer.

When we use a terminal loop at the remote end, it is important that the remote end's path between NNI ingress and UNI egress and back to NNI egress is not blocked by spanning-tree. If there is not link on UNI, spanning tree would otherwise block that forwarding path.

For facility loops, it is only important that spanning tree has not blocked NNI.

Also LLDP transmission may have to be disabled, especially if the EVC is untagged.

VLAN configuration-wise, we use an S-port for NNI (Gi 1/2) and a C-port for UNI (Gi 1/3) and disallow all VLANs. Even when all VLANs are disallowed, frames will get classified from the S-tag (if present) and forwarded to UNI through the ECE rules installed or facility MAC-looped. In case the NNI carries untagged EVCs, it is recommended to let NNI have a Port VLAN ID set to an unused VLAN (e.g. 4095) and configure the NNI port to tag all but the Port VLAN ID on NNI egress.

When using simulated customer traffic, it is - in many cases - important that the frames have the same PCP value in the outer tag when they egress NNI as when they ingressed NNI. The reason is that the rules installed on NNI ingress in the local end may match on PCP, and if the PCP value has changed when it returns, it may or may not hit the ECE that the Y.1564 software thinks it will hit.

This is not required when using Y.1731 as test traffic, since the S-tag's PCP is not used in the subscriber domain.

In order to (partly) ensure that frames have the same VLAN ID and PCP in its outer tag (S-tag) when it egresses NNI as when it ingressed NNI, we enable QoS ingress tag classification on both UNI and NNI and do a one-to-one mapping of <PCP, DEI> to <CoS, DP>.

Likewise, we set the QoS Tag Remarking mode to Mapped for both NNI and UNI, and do a one-to-one mapping from <CoS, DP> to <PCP, DEI>.

Finally, we create four loops:

- A facility MAC-loop on NNI in the port domain (for profiles where DST is OAM-aware is unchecked).
- A terminal OAM-loop in the EVC subscriber domain (for profiles where DST is OAM-aware is checked).
- A facility MAC-loop on NNI in the EVC domain (for profiles where `DST is OAM-aware` is unchecked).
- A terminal MAC-loop in the EVC subscriber domain (for profiles where `DST is OAM-aware` is unchecked).

The third loop is only for reference and will be kept disabled throughout this chapter.

The fourth loop cannot be applied in the configuration because it conflicts with the second loop, but we will use it in Partial Frame Loss, page 21-50.

Initially, we enable the first two loops, and keep the third disabled. This will cause traffic to loop at the first possible place, which in this case will be the MAC-loop on NNI.

This gives the following configuration (not entire configuration is shown):

```
evc policer  1 enable rate -type line cir  10000  cbs  10000  eir  25000  ebs  10000
evc policer  2 enable type single cir   75000  cbs  8000  eir  10000  ebs  4000
evc policer  3 enable mode coupled cir   50000  cbs  6000  eir  10000  ebs  6000
evc policer  4 enable cir  25000  cbs  2000  eir  10000  ebs  8000
evc  10  vid  1000  ivid  1234  interface GigabitEthernet   1/2  learning policer none
evc ece  1  interface Gi  1/3  outer-tag match type c -tagged vid  24  add pcp-mode fixed dei -mode dp pcp  5  tx-lookup pcp -vid evc  10  policer  1  cos  7  dpl  0
evc ece  2  interface Gi  1/3  outer-tag match type c -tagged vid  48  add pcp-mode mapped dei -mode dp tx -lookup pcp -vid evc  10  policer  2  cos  6  dpl  1
evc ece  3  interface Gi  1/3  outer-tag match type c -tagged add dei -mode dp evc  10  policer none pop  1  policer  3  cos  5
evc ece  4  interface Gi  1/3  outer-tag match type untagged add pcp  -mode fixed dei -mode dp pcp  7  tx-lookup pcp -vid evc  10  policer  4  cos  4

# NNI
interface GigabitEthernet   1/2
 no loop -protect
 switchport hybrid allowed vlan none
 switchport hybrid port  -type s -port
 switchport mode hybrid
 no lldp receive
 no lldp transmit
 qos trust tag
 qos map tag -cos pcp  0  dei  0  cos  0  dpl  0
 qos map tag -cos pcp  0  dei  1  cos  0  dpl  1
 qos map tag -cos pcp  1  dei  0  cos  1  dpl  0
 qos map tag -cos pcp  1  dei  1  cos  1  dpl  1
 qos tag -remark mapped
 qos map cos -tag cos  0  dpl  0  pcp  0  dei  0
 qos map cos -tag cos  0  dpl  1  pcp  0  dei  1
 qos map cos -tag cos  1  dpl  0  pcp  1  dei  0
 qos map cos -tag cos  1  dpl  1  pcp  1  dei  1
 no spanning -tree

# UNI
interface GigabitEthernet   1/3
 no loop -protect
 switchport hybrid allowed vlan none
 switchport hybrid ingress  -filtering
 switchport mode hybrid
 no lldp receive
 no lldp transmit
 qos trust tag
 qos map tag -cos pcp  0  dei  0  cos  0  dpl  0
 qos map tag -cos pcp  0  dei  1  cos  0  dpl  1
 qos map tag -cos pcp  1  dei  0  cos  1  dpl  0
 qos map tag -cos pcp  1  dei  1  cos  1  dpl  1
 qos tag -remark mapped
 qos map cos -tag cos  0  dpl  0  pcp  0  dei  0
 qos map cos -tag cos  0  dpl  1  pcp  0  dei  1
 qos map cos -tag cos  1  dpl  0  pcp  1  dei  0
 qos map cos -tag cos  1  dpl  1  pcp  1  dei  1
 no spanning -tree

traffic-test-loop 1 type mac -loop interface GigabitEthernet   1/2 direction facility domain port
traffic-test-loop 2 type oam -loop level  7 interface GigabitEthernet   1/3 direction terminal domain evc   10
traffic-test-loop 2 subscriber all
traffic-test-loop 3 type mac -loop interface GigabitEthernet   1/2 direction facility domain evc   10 admin-state disabled
# This is an example of a terminal MAC   -loop in the EVC domain  .
# It is not supported on all products   , and if enabled , it will collide with
# traffic -test-loop 2 above .
! traffic -test-loop 4 type mac -loop interface GigabitEthernet   1/3 direction terminal domain evc   10 subscriber all
```

Software Configuration

Time to go through the test report. The first part lists the used software version, board type, build date and on some products also a code revision. These properties are important in order to be able to reproduce and troubleshoot a failing test.

```
***************************************************************************** Y.1564 SAM
Test
*****************************************************************************
Software configuration:
  Version                      : <Software Version>
  Board                        : <Hardware Board>
  Build date                   : 2017-11-10T10:59:54+01:00
  Code revision                : <Not available in all products>
```

Profile and Report Configuration

The next part shows the common parameters of the chosen profile, including the type of test traffic and Y.1731 DM PDU types (Y.1731 DMM/Y.1731 1DM/None) along with the chosen parameters selected during start of test. The individual sub-test configurations are listed along with the actual execution of the tests.

```
Profile configuration:
  Profile name                : profile-OAM-unaware
  Description                 :
  Measurement type            : Single-ended (DST loops traffic)
  DST is OAM aware            : No
  Test traffic type           : Simulated customer traffic
  Test traffic SMAC           : 00-01-02-03-04-05
  Delay measurement type      : Y.1731 1DM
  MEG Level                   : 7
  Dwell time                  : 500 msecs
  Frame size                  : User-defined (EMIX=u)
  User-defined frame size     : 1000 bytes
  CIR configuration test      : Enabled
  EIR configuration test      : Enabled
  Traffic policing test       : Enabled
  Service performance test    : Enabled
  Acceptable FLR              : 0 permille
  Acceptable FTD              : Check disabled
  Acceptable FDV              : Check disabled

Report configuration:
  Report name                 : Report-6
  Description                 :
  Peer MAC                    : 00-01-c1-00-b5-33
  EVC ID                      : 10
  EVC VLAN ID                 : 1000
  ECE IDs on EVC              : 1 2 3 4
  ECE IDs under test          : 1 2 3 4
```

UNI and NNI Status

Next comes the configuration and status of UNI and NNI interfaces.

There doesn't have to be link on UNI ports for the switch to apply frames, but at least one NNI port needs to have link.

```
Configuration for UNI interface GigabitEthernet 1/3:
  Link state                  : Down
  Speed                       : 1000 Mbps
  MTU                         : 10240 bytes
  MAC                         : 00-01-c1-00-00-03

Configuration for NNI interface GigabitEthernet 1/2:
  Link state                  : Up
  Speed                       : 1000 Mbps
  MTU                         : 10240 bytes
```

Policer Configuration

Next comes policer configurations. All policers referenced by ECEs under test are listed. For each policer, an ECE use count is shown. In the following example, it says `1/1` for all policers, because one given policer is only used by one ECE (the last `1` in `1/1`) and because all ECEs are under test (the first `1` in `1/1`).

```
Configuration for Policer ID 1:
  ECE use count               : 1/1
  CIR/EIR                     : 100.000/25.000 Mbps
  CBS/EBS                     : 10000/10000 bytes
  Rate Type                   : Layer 1 (line)
  Policer Type                : Color Aware

Configuration for Policer ID 2:
  ECE use count               : 1/1
  CIR/EIR                     : 75.000/0.000 Mbps
  CBS/EBS                     : 8000/0 bytes
  Rate Type                   : Layer 2 (data)
  Policer Type                : Color Blind - Single Leaky Bucket
  Warning                        : The hardware may burst up to eight frames per
                               flow in order to achieve a given rate.
                              : Since CBS is less than eight times the frame
                                size, the flow going into this single leaky
                                bucket
                              : policer that would retain its color in a non-
                                bursty flow may get painted discarded,
                                causing a lower in-service rate.

Configuration for Policer ID 3:
  ECE use count               : 1/1
  CIR/EIR                     : 50.000/10.000 Mbps
  CBS/EBS                     : 6000/6000 bytes
  Rate Type                   : Layer 2 (data)
  Policer Type                : Color Aware - Coupled
  Warning                     : The hardware may burst up to eight frames per
                               flow in order to achieve a given rate.
                             : Since CBS is less than eight times the frame
                               size, some green frames that would remain
                               green
                             : in a non-bursty flow may get painted yellow,
                               causing a lower green in-service rate.
                             : Since EBS is less than eight times the frame
                               size, some yellow frames that would remain
                               yellow
                                     : in a non-bursty flow may get discarded (painted
                               red), causing a lower yellow in-service
                              rate.

Configuration for Policer ID 4:
  ECE use count               : 1/1
  CIR/EIR                     : 25.000/10.000 Mbps
  CBS/EBS                     : 2000/8000 bytes
  Rate Type                   : Layer 2 (data)
  Policer Type                : Color Aware
  Warning                        : The hardware may burst up to eight frames per
                               flow in order to achieve a given rate.
                              : Since CBS is less than eight times the frame
                                size, some green frames that would remain
                                green
                                : in a non-bursty flow may get painted yellow,
                               causing a lower green in-service rate.
```

The hardware frame generator for VSC7418 exhibits some inexpedient properties. In order to achieve requested rates, it must be configured to send the same frame multiple times. This has two unfortunate side-effects:

- It is not always possible to achieve the requested rate. The closest, lower, possible rate will be chosen. The achievable rate may be several Mbps off the desired rate.
- Up to eight frames may be sent in a burst. This may cause the policer to paint green frames that normally would remain green (in a CIR Configuration Test, for instance) yellow or discard yellow frames that normally would have remained yellow. When the policer's burst size is smaller than eight times the frame size, a warning will be displayed under the policer configuration, as shown in the example above for policer #2, #3, and #4. In order for this not to be displayed, both CBS and EBS must be greater than `8 * (possible_ifg_and_preamble + selected_frame_size + sizeof(C-tag))`. `possible_ifg_and_preamble` is 20 bytes (for IFG and preamble) if the policer's `Rate Type` is `Layer 1 (line)`, and 0 bytes if it is `Layer 2 (data)`.

ECE Configuration and Resolved Values

All ECEs of the EVC are listed in the order they are added to hardware.

For each ECE, it shows whether it is selected for test, and a section that shows the most important fields of what the ECE matches on UNI ingress.

The Matching section is followed by a section showing the most important configured actions for the ECE.

Finally, if the ECE is under test, the Y.1564 software prints a section called Resolutions. The first field in this section shows the selected UNI. If the user asked the Y.1564 software to auto-pick a UNI, the interface name is followed by (Auto). The same goes for VLAN ID and PCP.

The PCP of NNI Outer Tag shows the computed PCP value in the S-tag on NNI or None for untagged EVCs. This computation is not straight forward, and may depend on the configuration of other ECEs in this EVC and on QoS Egress Tag Remarking configuration on NNI.

In many cases, it is of utmost importance that the remote end does not alter the PCP value in the S-tag during looping, since the Y.1564 software expects it to have the same value when it returns to NNI ingress, in order to further analyze where it counts.

```
Configuration for ECE ID 1:
  Under test                 : Yes
  Matching                   :
    Outer VLAN Tag Type       : C-tagged only
    Inner VLAN Tag Type       : Any
    Frame Type                : Any
  Actions                    :
    Tx Lookup                 : VID-PCP
    Policer ID                : 1
    Tag Pop Count             : 0
    CoS                       : 7
    Drop Precedence           : Forced to green
    Egress Outer Tag PCP Mode : Fixed (5)
  Resolutions                :
    UNI interface             : GigabitEthernet 1/3 (Auto)
    PCP of NNI Outer Tag      : 5
    VLAN ID                   : 24 (Auto)
    PCP                       : 0 (Auto)
    Green flow                : DEI = 0 (Auto)
    Yellow flow               : Inactive (Unable to generate yellow flow into policer,
because the ECE's Drop Precedence is
                                forced to green)
    DSCP                        : N/A
    Frame size                  : 1004 bytes
    Frame                       : 00 01 c1 00 b5 33 00 01  02 03 04 05 81 00 00 18
                                : 88 80 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                                : 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                                : 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                                : ...
                                : 00 00 00 00 00 00 00 0a  00 00 00 01 xx xx xx xx

Configuration for ECE ID 2:
  Under test                    : Yes
  Matching                      :
    Outer VLAN Tag Type         : C-tagged only
    Inner VLAN Tag Type         : Any
    Frame Type                  : Any
  Actions                       :
    Tx Lookup                   : VID-PCP
    Policer ID                  : 2
    Tag Pop Count               : 0
    CoS                         : 6
    Drop Precedence             : Forced to yellow
    Egress Outer Tag PCP Mode : Mapped
  Resolutions                   :
    UNI interface               : GigabitEthernet 1/3 (Auto)
    PCP of NNI Outer Tag        : 6
    VLAN ID                     : 48 (Auto)
    PCP                         : 0 (Auto)
    Green flow                  : Inactive (Unable to generate green flow into policer,
because the ECE's Drop Precedence is
                                  forced to yellow)
    Yellow flow                 : DEI = 1 (Auto)
    DSCP                        : N/A
    Frame size                  : 1004 bytes
    Frame (yellow)              : 00 01 c1 00 b5 33 00 01  02 03 04 05 81 00 10 30
                                : 88 80 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                                : 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                                : 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                                : ...
                                : 00 00 00 00 00 00 00 0a  00 00 00 02 xx xx xx xx

Configuration for ECE ID 3:
  Under test                    : Yes
  Matching                      :
    Outer VLAN Tag Type         : C-tagged only
    Inner VLAN Tag Type         : Any
    Frame Type                  : Any
  Actions                       :
    Tx Lookup                   : VID
    Policer ID                  : 3
    Tag Pop Count               : 1
    CoS                         : 5
    Drop Precedence             : From basic classification
    Egress Outer Tag PCP Mode : Classified
  Resolutions                   :
    UNI interface               : GigabitEthernet 1/3 (Auto)
    PCP of NNI Outer Tag        : 5
    VLAN ID                     : 1 (Auto)
    PCP                         : 0 (Auto)
    Green flow                  : DEI = 0 (Auto)
    Yellow flow                 : DEI = 1 (Auto)
    DSCP                        : N/A
    Frame size                  : 1004 bytes
    Frame (green)               : 00 01 c1 00 b5 33 00 01  02 03 04 05 81 00 00 01
                                : 88 80 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

```
                              : 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                              : 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                              : ...
                              : 00 00 00 00 00 00 00 0a  00 00 00 03 xx xx xx xx
    Frame (yellow)            : 00 01 c1 00 b5 33 00 01  02 03 04 05 81 00 10 01
                              : 88 80 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                              : 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                              : 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                              : ...
                              : 00 00 00 00 00 00 00 0a  00 00 00 03 xx xx xx xx

Configuration for ECE ID 4:
  Under test                  : Yes
  Matching                    :
    Outer VLAN Tag Type       : Untagged only
    Inner VLAN Tag Type       : Any
    Frame Type                : Any
  Actions                     :
    Tx Lookup                 : VID-PCP
    Policer ID                : 4
    Tag Pop Count             : 0
    CoS                       : 4
    Drop Precedence           : From basic classification
    Egress Outer Tag PCP Mode : Fixed (7)
  Resolutions                 :
    UNI interface             : GigabitEthernet 1/3 (Auto)
    PCP of NNI Outer Tag      : 4
    VLAN ID                   : Untagged (Auto)
    PCP                       : N/A
    DEI                       : N/A
    Flow Color                : Green
    DSCP                      : N/A
    Frame size                : 1000 bytes
    Frame                     : 00 01 c1 00 b5 33 00 01  02 03 04 05 88 80 00 00
                              : 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                              : 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                              : 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
                              : ...
                              : 00 00 00 00 00 00 00 0a  00 00 00 04 xx xx xx xx
```

The Y.1564 software also analyzes whether it can generate both a green and a yellow flow. This depends on the ECE's configuration along with the UNI port's QoS settings.

In the example above, it's not possible to generate a yellow flow for ECE #1, because its Action's Drop Precedence is set to 0, causing all frames to be green when they hit the policer. Likewise, it's not possible to generate a green flow for ECE #2, because its Action's Drop Precedence is set to 1.

ECE #3 is tagged and QoS tag classification is enabled on UNI, so the color of the flow can be controlled with the DEI bit.

ECE #4 is untagged, and therefore it is the UNI port's QoS default classification that determines the color of the flow when it hits the policer. In this example, the default DP value is 0, causing the flow color to be green.

If using Simulated Customer traffic, the one or two frames it will use to test an ECE are printed. The two four-byte values coming just before the FCS (xx xx xx xx) are EVC ID and ECE ID, respectively – in network order. These can be used to identify the traffic on the wire.

If using Y.1731 traffic, the test frames will not be shown.

Table Legends

Each sub-test will produce one or two tables with results. The columns of these tables are explained in the table legends section of the report. The first table legend explains the test traffic table, the second explains the DM table. The test traffic table legend changes slightly depending on the test traffic type. The below example shows the table legend for simulated customer traffic.

```
Test Results table legend  :
  UNI Ingr ECE                : The ECE ID for which the rest of this row pertains
  UNI Egr ECE                 : The ECE that counts looped traffic for the corresponding UNI Ingr ECE
  UNI Ing CoS                 : Class of Service that UNI ingress traffic on this ECE maps to
  Color /Step  #              : Color of frame flow   (G = Green , Y = Yellow ) and step number in CIR configuration test
  Color                       : Color of frame flow
  Under Test                  : Indicates whether this ECE was selected to be tested when the test was initiated
  UNI Ingr , Requested        : Requested traffic rate on UNI   , in Line Rate  (L1) and Data Rate  (L2 )
  UNI Ingr , Applied          : Hardware doesn 't always support the requested rate   . This is the rate that hardware
                              : tells software it supports given the requested rate
  UNI Ingr , In-service       : The rate and frame count after policing on the UNI    . This is the rate supposed to egress NNI   .
                              : Notice , that this rate may be somewhat lower than what is expected given the policer     's
                              : configuration and applied rate   . The reason for this is that the hardware may burst up
                              : to eight frames per flow in order to achieve a given rate    . This may not pose a problem
                              : if the policer 's CBS /EBS is configured to absorb these bursts   , that is , set to values
                              : that are at least eight times the test frame size    . If not , green frames may be painted
                              : yellow /red and yellow frames may be painted red    (discarded ) when passing through the
                              : policer . The net -effect is in -service rates that are lower than anticipated   , and the
                              : yellow counters may count on pure green traffic at CIR or below    . If this situation occurs  ,
                              : a warning will be displayed under the relevant policer    's configuration section in this
                              : report .
  UNI Egr                     : Actual NNI ->UNI frame count after looping   (may be  0 if counted on another ECE  )
  Frame Loss                  : Percentage of frames lost between UNI ingress and UNI egress
  Status                      : PASS , SKIP, FAIL or empty if not under test

Delay Measurements table legend  :
  UNI Ing CoS                 : Class of Service that UNI ingress traffic on the ECEs under test maps to
  UNI Egr CoS                 : Class of Service that counts looped DM traffic for the corresponding UNI ingress CoS
  Under Test                  : Indicates whether an ECE mapping to this ingress CoS is under test
  Step  #                     : Step number in CIR configuration test
  UNI Ingr                    : Number of DM frames ingressing UNI    (transmitted by local end  )
  UNI Egr                     : Number of DM frames egressing UNI    (received from remote end  )
  Min /Avg/Max Delay          : Minimum , average , and maximum delay seen on the DM frames
  Min /Avg /Max Delay Var .  : Minimum , average , and maximum delay variation seen on the DM frames
  Status                      : PASS or FAIL  - only for CoSs under test
```

Overall Status

The last section before actual test results contain an overall status of the test. It includes test start and end time and whether the test succeeded or failed. Here is an example:

```
Overall execution status:
  Started at                 : 1970-01-01T03:19:02+00:00
  Ended at                   : 1970-01-01T03:19:13+00:00
  Status                     : Succeeded (at least one trial was skipped)
```

As we shall see later, it may be that not all ECEs can be tested in all sub-tests, for instance because only a yellow flow can be generated on a color-aware policer in the CIR configuration test. In that case, the testing of that particular ECE will be skipped, and the overall status will become Succeeded (at least one trial was skipped). If all ECEs under test are tested in all sub-tests, Status will be Succeeded. If at least one test fails, Status will be Failed.

CIR Configuration Test Results

This part of the test report shows the configuration and status of executing the CIR configuration test followed by the actual test results.

```
****************CIR configuration test **************************
Configuration:
  Duration per step          : 1 second
  Delay meas. interval       : 400 msecs
  Step count                 : 2
```

```
Status:
  Started at                  : 1970-01-01T03:19:02+00:00
  Ended at                    : 1970-01-01T03:19:05+00:00
  Status                      : Succeeded
```

When using Simulated Customer traffic as test traffic, the test results table has two rows for every ECE under test, but also ECEs not under test may be shown if their counters are non-zero or if the ECE captures looped traffic. This means that one can assume that ECEs that are not displayed have their counters steady at zero.

The first column shows the UNI ingress ECE ID. The Y.1564 software computes the ECE ID the traffic is supposed to egress on when it has returned from the remote end – provided the PCP value in the S-tag is preserved from NNI egress to NNI ingress. This is shown in the second column. The CoS into which it is forced upon UNI ingress is shown in the third column. The fourth column shows the Color and the Step number. In this particular example, the number of CIR Configuration Test steps is reduced to 2 from the default of 4. G stands for Green and Y stands for Yellow traffic.

The Under Test column is self-explanatory, and the UNI Ingr (L1/L2) Requested column shows the rate measured in Mbps that software has requested the hardware frame generator to produce. The hardware frame generator may not be able to fulfil the request, so the next column shows what it actually was able to produce – also measured in Mbps.

The two UNI Ingr In-Service columns show the rate and number of frames as read in hardware after the UNI ingress traffic has passed through the policer.

The Frame Loss column shows the frame losses (in percent), but only for ECEs that actually are expected to count UNI egress traffic.

The last column shows whether test of the ECE passes, fails, or is skipped. Only test of green traffic can fail.

```
Test Results :
---- ---- --- ------ ----- -----------------  -----------------  -----------------  ------------  ------------  ------  ------
UNI  UNI  UNI Color / Under UNI Ingr  (L1/L2)  UNI Ingr  (L1/L2)  UNI Ingr  (L1/L2)  UNI Ingr      UNI Egr       Frame  Status
Ingr Egr  Ing Step  # Test  Requested         Applied           In   -service        In -service                 Loss
ECE  ECE  CoS               [Mbps]            [ Mbps]           [ Mbps]            [ Frames]     [ Frames]      [%]
---- ---- --- ------ ----- -----------------  -----------------  -----------------  ------------  ------------  ------  ------
   1    1   7  G/1    Yes       50.000/49.023     49 .995/49.019     49 .581/48.612          6113          9228  0  .00  PASS
   1    1   7  Y/1    Yes                                             0.000/0.000             0             0         PASS
   2    2   6  G/1    Yes                                             0.000/0.000             0          1535  0  .00  PASS
   2    2   6  Y/1    Yes       38.247/37.500     37 .756/37.019     37 .415/36.684          4613          4613  0  .00  PASS
   3    1   5  G/1    Yes       25.498/25.000     25 .492/24.995     25 .265/24.771          3115             0         PASS
   3    1   5  Y/1    Yes                                             0.000/0.000             0             0         PASS
   4    2   4  G/1    Yes       12.750/12.500     12 .484/12.240     12 .525/12.279          1535             0         PASS
   4    2   4  Y/1    Yes                                             0.000/0.000             0             0         PASS
   1    1   7  G/2    Yes      100.000/98.046     99 .990/98.038     99 .762/97.813         12178         18376  0  .00  PASS
   1    1   7  Y/2    Yes                                             0.000/0.000             0             0         PASS
   2    2   6  G/2    Yes                                             0.000/0.000             0          3107  0  .00  PASS
   2    2   6  Y/2    Yes       76.494/75.000     76 .487/74.994     76 .275/74.785          9311          9314  0  .00  PASS
   3    1   5  G/2    Yes       50.996/50.000     50 .954/49.959     50 .774/49.782          6198             0         PASS
   3    1   5  Y/2    Yes                                             0.000/0.000             0             0         PASS
   4    2   4  G/2    Yes       25.500/25.000     25 .483/24.984     25 .353/24.855          3107             0         PASS
   4    2   4  Y/2    Yes                                             0.024/0.023             3             0         PASS
```

In the example, the Y.1564 software expects frames that match ECE #1 and frames that match ECE #3 to count in ECE #1 when they egress UNI again. This can also be seen on the counters, where the `UNI Egr` frame counters for ECE #1 is the sum of the `UNI Ingr` frame counters of ECE #1 and #3. The same goes for ECE #2 and ECE #4, which both count in ECE#2 on UNI egress.

Another important thing to notice is the applied traffic for ECE #2: Remember from the ECE and policer configuration sections that ECE #2 has DP forced to 1, that is, all traffic is considered yellow when it hits the policer. If the policer had been a color-aware policer, it would not have been possible to conduct the CIR configuration test for ECE #2, because yellow traffic into a color-aware policer will be handled by the yellow bucket, which is configured with EIR and EBS and not with CIR and CBS. In this particular configuration, the policer belonging to ECE #2 is a single leaky bucket policer, which - by nature – is color blind and configured with CIR and CBS, only. The color of the frames on the other side of the policer is either the color it had when ingressing the policer or red, which are discarded. In this case, we transmit yellow frames into the policer, so the ones that come through the policer are still yellow. Since the ITU-T Y.1564 Recommendation forbids failing on yellow frames, such a test can never fail – even if 0 of the 4613 yellow frames in step 1 return to the local end.

A final note on the test results in on ECE #4, which uses Policer #4: Remember from the Policer configuration section that Policer #4 had a warning indicating that some green frames may get painted yellow by the policer if the flow is bursty. In this case, it appears that the burstiness of the ingress flow causes 3 green frames to become yellow (step 2) as they pass through the policer. The same warning appears for ECE #3, but the number of yellow frames through that policer is zero. This is because the number of frames needed to generate the requested rate is smaller than the burst size divided by the frame size for ECE #3.

The delay measurements are presented in its own table:

```
Delay Measurements:
--- --- ------ ----- -------- -------- ----------------- ----------------- ------
UNI UNI Step # Under UNI Ingr UNI Egr  Min/Avg/Max       Min/Avg/Max       Status
Ing Egr        Test                    Delay             Delay Var.
CoS CoS              [Frames] [Frames] [usecs]           [usecs]
--- --- ------ ----- -------- -------- ----------------- ----------------- --
  4   4      1 Yes          2        4          11/11/11             0/0/0 PASS
  5   4      1 Yes          2        0                                     PASS
  6   6      1 Yes          2        2          11/26/41          29/29/29 PASS
  7   7      1 Yes          2        2          11/30/48          36/36/36 PASS
  4   4      2 Yes          2        4          11/19/43           0/21/32 PASS
  5   4      2 Yes          2        0                                     PASS
  6   6      2 Yes          2        2          11/11/12             0/0/0 PASS
  7   7      2 Yes          2        2          11/11/11             0/0/0 PASS
```

Delay measurements are made per CoS, and not per ECE. If multiple ECEs under test map to the same CoS, only one set of DM is made for that CoS. In our example, all four ECEs map to different CoSs, so we get four sets of delay measurements.
The first column is the CoS the 1DM/DMM frames hit on UNI ingress, and the second is the CoS that the Y.1564 software expects the looped traffic to count on. Looped DM frames are redirected to the CPU, where they are further analyzed and the results are stored per CoS. The report contains a row per CoS if under test and additional CoS rows if the DM counters are non-zero for that particular CoS. This serves to ease debugging in case the test fails. The third column is the step number (only present in CIR configuration test), and the fourth column shows whether the CoS is under test or not. The fifth and sixth columns hold the number of UNI Ingressed and UNI egressed frames. The seventh and eighth columns show the measured frame transfer delay and the delay variation, measured in microseconds. Finally, the ninth column shows whether everything is as expected (PASS/FAIL).

Testing the same EVC with profile-OAM-aware (remember to disable traffic-test-loop #1 at the remote end) yields the following results:

```
Test Results :
---- --- --- ------ ----- ----------------- ----------------- ----------------- ------------ ------------ ------ ------
ECE  UNI UNI Color / Under UNI Ingr  (L1/L2)  UNI Ingr  (L1/L2)  UNI Ingr  (L1/L2)  UNI Ingr     UNI Egr      Frame  Status
ID   Ing Egr Step  # Test  Requested         Applied           In   -service       In -service               Loss
     CoS CoS               [Mbps ]           [ Mbps]           [ Mbps]          [ Frames ]   [ Frames ]    [%]
---- --- --- ------ ----- ----------------- ----------------- ----------------- ------------ ------------ ------ ------
   4   4   4 G/1    Yes        12.750/12.500     12 .484/12.240     12 .484/12.239        1530         4639   0  .00 PASS
   4   4   4 Y/1    Yes                                                0.000/0.000           0            0          PASS
   3   5   4 G/1    Yes        25.498/25.000     25 .493/24.995     25 .468/24.970        3109            0          PASS
   3   5   4 Y/1    Yes                                                0.000/0.000           0            0          PASS
   2   6   6 G/1    Yes                                                0.000/0.000           0            0          PASS
   2   6   6 Y/1    Yes        38.247/37.500     37 .756/37.019     37 .658/36.922        4597         4597   0  .00 PASS
   1   7   7 G/1    Yes        50.000/49.023     49 .995/49.019     49 .823/48.849        6082         6082   0  .00 PASS
   1   7   7 Y/1    Yes                                                0.000/0.000           0            0          PASS
   4   4   4 G/2    Yes        25.500/25.000     25 .483/24.984     25 .442/24.943        3118         9322   0  .00 PASS
   4   4   4 Y/2    Yes                                                0.008/0.007           1            1   0  .00 PASS
   3   5   4 G/2    Yes        50.996/50.000     50 .954/49.959     50 .823/49.830        6204            0          PASS
   3   5   4 Y/2    Yes                                                0.000/0.000           0            0          PASS
   2   6   6 G/2    Yes                                                0.000/0.000           0            0          PASS
   2   6   6 Y/2    Yes        76.494/75.000     76 .488/74.994     76 .210/74.721        9303         9303   0  .00 PASS
   1   7   7 G/2    Yes       100.000/98.046     99 .991/98.038     99 .500/97.556       12146        12146   0  .00 PASS
   1   7   7 Y/2    Yes                                                0.000/0.000           0            0          PASS

Delay Measurements  :
--- --- ------ ----- -------- -------- -----------------  -----------------  ------
UNI UNI Step  # Under UNI Ingr UNI Egr  Min  /Avg/Max       Min /Avg/Max       Status
Ing Egr        Test                    Delay              Delay Var    .
CoS CoS               [Frames ] [Frames ] [usecs ]           [ usecs ]
--- --- ------ ----- -------- -------- -----------------  -----------------  ------
  4   4      1  Yes          1        2          13  /13/13              0  /0/0  PASS
  5   4      1  Yes          1        0                                       PASS
  6   6      1  Yes          1        1          14  /14/14              0  /0/0  PASS
  7   7      1  Yes          1        1          14  /14/14              0  /0/0  PASS
  4   4      2  Yes          1        2          13  /13/14              0  /0/0  PASS
  5   4      2  Yes          1        0                                       PASS
  6   6      2  Yes          1        1          14  /14/14              0  /0/0  PASS
  7   7      2  Yes          1        1          13  /13/13              0  /0/0  PASS
```

Here, it is actually CoSs that are tested rather than ECEs. The reason is that alternate rules that capture Y.1731 OAM traffic are installed per CoS under test on SRC. If one attempts to start a Y.1564 test with two or more ECEs that map to the same CoS while using Y.1731 test traffic, the start is refused.

The first column is the ECE ID and the two following are the CoS the Y.1731 traffic is forced into on UNI ingress followed by the CoS it is expected to count in on UNI egress. The remaining columns are identical to those from the Customer Simulated test.

There will be two rows per CoS under test – one for green and one for yellow traffic.

With the given ECE configuration, the Y.1564 software expects ingress traffic on CoS 4 and CoS 5 to test on CoS 4 and the remaining two to count on their own CoS. In fact, only when an ECE is untagged or a possible C-tag gets stripped before the frame exits NNI, will there be a non-one-to-one mapping between ingress and egress CoS.

The rates applied are identical to those from the simulated customer report, but the number of frames may vary slightly because the flows are started and stopped by software.

The DM table is similar to that from the simulated customer report.

EIR Configuration Test Results

The EIR configuration test is a test that only executes on dual leaky bucket policers, so if an ECE's policer is a single leaky bucket policer, test of that ECE is skipped. As described in EIR Configuration Test, page 21-11, there may be other reasons to skip the EIR configuration test.

The following shows the test configuration, status, and results of executing the EIR configuration test that uses the profile-OAM-unaware profile.

```
************************************************    EIR configuration test   ************************************************
 Configuration :
  Duration                      : 1 second
  Delay meas . interval         : 400 msecs

Status :
  Started at                    : 1970 -01- 01T03 :19:05+00:00
  Ended at                      : 1970 -01- 01T03 :19:06+00:00
  Status                        : Succeeded  (at least one trial was skipped  )
  ECE ID  1 skip reason         : Unable to generate yellow flow into policer   , because the ECE 's Drop Precedence is forced to
                                  green
  ECE ID  2 skip reason         : Policer is a single leaky bucket policer with no EIR
  ECE ID  4 skip reason         : Unable to generate yellow flow into policer   , because the UNI port 's default QoS settings mark
                                  the frame green

Test Results :
---- ---- --- ------ ----- -----------------  -----------------  -----------------  ------------  ------------  ------  ------
UNI  UNI  UNI Color  Under UNI Ingr   (L1/L2)  UNI Ingr  (L1/L2)  UNI Ingr  (L1/L2)  UNI Ingr     UNI Egr       Frame  Status
Ingr Egr  Ing        Test  Requested          Applied           In    -service        In -service                Loss
ECE  ECE  CoS               [Mbps]            [ Mbps ]           [ Mbps ]          [ Frames ]    [ Frames ]     [%]
---- ---- --- ------ ----- -----------------  -----------------  -----------------  ------------  ------------  ------  ------
   1    1   7 Green  Yes                                                0.000/0.000            0          6210   0   .00 SKIP
   1    1   7 Yellow Yes                                                0.000/0.000            0          1211   0   .00 SKIP
   2    2   6 Green  Yes                                                0.000/0.000            0             0            SKIP
   2    2   6 Yellow Yes                                                0.000/0.000            0             0            SKIP
   3    1   5 Green  Yes       50.996/50.000     50 .954/49.959     50 .872/49.878         6210             0            PASS
   3    1   5 Yellow Yes       10.199/10.000      10 .157/9.959      9 .920/9.726          1211             0            PASS
   4    2   4 Green  Yes                                                0.000/0.000            0             0            SKIP
   4    2   4 Yellow Yes                                                0.000/0.000            0             0            SKIP

Delay Measurements :
--- --- ----- -------- -------- -----------------  -----------------  ------
UNI UNI Under UNI Ingr UNI Egr  Min   /Avg/Max       Min /Avg/Max       Status
Ing Egr Test                    Delay             Delay Var    .
CoS CoS       [Frames] [Frames] [usecs]             [ usecs]
--- --- ----- -------- -------- -----------------  -----------------  ------
  4   4 Yes          2        4          11  /12/12             0 /0/0 PASS
  5   4 Yes          2        0                                        PASS
  6   6 Yes          2        2          12  /12/12             0 /0/0 PASS
  7   7 Yes          2        2          12  /12/12             0 /0/0 PASS
```

Only ECE #3 fulfills the requirements for performing an EIR configuration test; the remaining three ECEs are skipped, and therefore marked as such.

ECE #1 is skipped because only a green flow can be generated into a color-aware policer.

ECE #2 is skipped because it uses a single leaky bucket policer.

ECE #4 is skipped because it is an untagged ECE where the color of the flow cannot be chosen. In this example, the UNI default QoS settings will mark all frames as green.

On ECE #3 both a green and a yellow flow is generated according to the policer's CIR and EIR. Notice that the frames are counted in ECE #1 when they return from remote end. This is why the `Frame Loss` is shown for ECE #1 and not ECE #3.

Delay measurements can be performed on all four ECEs (CoSs), because special rules are installed on the fly to capture this traffic, which bypasses ingress policers.

A common failure reason of the EIR configuration test is “Received more green frames than were transmitted”. Refer to the troubleshooting chapter (chapter Troubleshooting) for details on this.

Traffic Policing Test Results

The traffic policing test is similar to the EIR configuration test except that a larger yellow frame rate is applied compared to the EIR configuration test, and it is possible to test ECEs that use a single leaky bucket policer, where EIR is 0, as shown below, where ECE #2 is now testable with a yellow flow at 125% CIR.

```
************************************************    Traffic policing test   *************************************************
 Configuration :
  Duration                     : 1 second
  Delay meas . interval        : 400 msecs

Status :
  Started at                   : 1970 -01 - 01T03 :19 :06+00 : 00
  Ended at                     : 1970 -01 - 01T03 :19 :08+00 : 00
  Status                       : Succeeded  (at least one trial was skipped  )
  ECE ID 1 skip reason         : Unable to generate yellow flow into policer   , because the ECE 's Drop Precedence is forced to
green
  ECE ID 4 skip reason         : Unable to generate yellow flow into policer   , because the UNI port 's default QoS settings mark
the frame green

Test Results :
---- ---- --- ------ ----- -----------------  -----------------  -----------------  ------------  ------------  ------ ------
UNI  UNI  UNI Color  Under UNI Ingr   (L1/L2)  UNI Ingr  (L1/L2)  UNI Ingr  (L1/L2)  UNI Ingr      UNI Egr       Frame  Status
Ingr Egr  Ing        Test  Requested         Applied           In    -service         In -service                 Loss
ECE  ECE  CoS               [Mbps]            [ Mbps ]           [ Mbps ]            [ Frames ]    [ Frames ]     [%]
---- ---- --- ------ ----- -----------------  -----------------  -----------------  ------------  ------------  ------ ------
   1    1   7 Green  Yes                                              0.000/0.000             0          6205   0   .00 SKIP
   1    1   7 Yellow Yes                                              0.000/0.000             0          1254   0   .00 SKIP
   2    2   6 Green  Yes                                              0.000/0.000             0             0           PASS
   2    2   6 Yellow Yes       95.617/93.750     85 .990/84.311     76 .398/74.905          9326          9326   0   .00 PASS
   3    1   5 Green  Yes       50.996/50.000     50 .954/49.959     50 .831/49.838          6205             0           PASS
   3    1   5 Yellow Yes       22.948/22.500     19 .659/19.276     10 .272/10.071          1254             0           PASS
   4    2   4 Green  Yes                                              0.000/0.000             0             0           SKIP
   4    2   4 Yellow Yes                                              0.000/0.000             0             0           SKIP

Delay Measurements :
--- --- ----- -------- -------- -----------------  -----------------  ------
UNI UNI Under UNI Ingr UNI Egr  Min  /Avg/Max        Min /Avg/Max       Status
Ing Egr Test                    Delay              Delay Var   .
CoS CoS       [Frames] [Frames] [usecs]             [ usecs ]
--- --- ----- -------- -------- -----------------  -----------------  ------
  4   4 Yes          2        4         11  /22/36           7 /16/24 PASS
  5   4 Yes          2        0                                       PASS
  6   6 Yes          2        2         11  /11/11             0 /0/0 PASS
  7   7 Yes          2        2         11  /11/11             0 /0/0 PASS
```

Delay measurements are identical to the previous sub-tests.

Normally when the CIR and EIR configuration tests pass, the traffic policer test is likely to pass too.

Service Performance Test Results

The service performance test validates the quality of the service over time up to 24 hours. The test rates and flow colors are identical to the last step of the CIR configuration test.

```
************************************************    Service performance test   ************************************************
 Configuration :
  Duration                     : 5 seconds
  Delay meas . interval        : 400 msecs

Status :
  Started at                   : 1970 -01 - 01T03 :19 :08+00 : 00
  Ended at                     : 1970 -01 - 01T03 :19 :13+00 : 00
  Status                       : Succeeded

Test Results :
---- ---- --- ------ ----- -----------------  -----------------  -----------------  ------------  ------------  ------ ------
UNI  UNI  UNI Color  Under UNI Ingr   (L1/L2)  UNI Ingr  (L1/L2)  UNI Ingr  (L1/L2)  UNI Ingr      UNI Egr       Frame  Status
Ingr Egr  Ing        Test  Requested         Applied           In    -service         In -service                 Loss
ECE  ECE  CoS               [Mbps]            [ Mbps ]           [ Mbps ]            [ Frames ]    [ Frames ]     [%]
---- ---- --- ------ ----- -----------------  -----------------  -----------------  ------------  ------------  ------ ------
   1    1   7 Green  Yes      100.000/98.046     99 .990/98.038     99 .929/97.977         60992         92065   0   .00 PASS
   1    1   7 Yellow Yes                                              0.000/0.000             0             0           PASS
   2    2   6 Green  Yes                                              0.000/0.000             0         15586   0   .00 PASS
   2    2   6 Yellow Yes       76.494/75.000     76 .487/74.994     76 .432/74.939         46651         46666   0   .00 PASS
   3    1   5 Green  Yes       50.996/50.000     50 .954/49.959     50 .910/49.915         31073             0           PASS
   3    1   5 Yellow Yes                                              0.000/0.000             0             0           PASS
   4    2   4 Green  Yes       25.500/25.000     25 .483/24.984     25 .436/24.937         15586             0           PASS
   4    2   4 Yellow Yes                                              0.024/0.023            15             0           PASS

Delay Measurements :
--- --- ----- -------- -------- -----------------  -----------------  ------
UNI UNI Under UNI Ingr UNI Egr  Min  /Avg/Max        Min /Avg/Max       Status
Ing Egr Test                    Delay              Delay Var   .
CoS CoS       [Frames] [Frames] [usecs]             [ usecs ]
--- --- ----- -------- -------- -----------------  -----------------  ------
  4   4 Yes         12       24         11  /18/48            0 /7/36 PASS
  5   4 Yes         12        0                                       PASS
  6   6 Yes         12       12         11  /21/50           0 /20/37 PASS
  7   7 Yes         12       12         11  /29/49           0 /26/38 PASS
```

Delay measurements are identical to the previous sub-tests.

Overall Result

The very last part of the report contains a summary of the entire test and is more or less a copy of overall status from Overall Status.

```
************************ Overall Result***************************
Ended at                    : 1970-01-01T03:19:13+00:00
Status                      : Succeeded (at least one trial was skipped)
****************************************************************************
```

Troubleshooting

If just one of the sub-tests fail, the whole test is stopped with a status of FAIL.

Execution of the CIR configuration test captures most erroneous configurations, and the results from that test are often the only information that can be used for troubleshooting possible issues.

Many configuration errors of the local end are caught by the Y.1564 software when the user attempts to start the test, that is, prior to actually executing the test. Examples of such configuration errors are:

Spanning Tree is discarding on either UNI or NNI

There is no link on NNI

Lack or wrongly configured QoS on NNI, etc.

Some cases, however are not or cannot be detected by the Y.1564 software. In the following we show examples of common situations you might come across, along with recommended techniques that might be helpful to root cause a failing test.

UNI Ingress Frame Count is Zero

The following shows an example where 50 Mbps of traffic is applied at UNI to ECE #1, but the test fails with “Delay Measurements: Acceptable frame loss exceeded”.

```
Status :
  Started at                  : 1970-01-03T23:15:34+00:00
  Ended at                    : 1970-01-03T23:15:36+00:00
  Status                      : Failed
  Details                     : Delay Measurements  : Acceptable frame loss exceeded

Test Results :
---- ---- --- ------ ----- ----------------- ----------------- ----------------- ------------ ------------ ------ ------
UNI  UNI  UNI Color / Under UNI Ingr  (L1/L2)  UNI Ingr  (L1/L2)  UNI Ingr  (L1/L2)  UNI Ingr     UNI Egr      Frame  Status
Ingr Egr  Ing Step  # Test  Requested          Applied          In   -service        In -service               Loss
ECE  ECE  CoS               [Mbps]             [ Mbps ]          [ Mbps ]            [ Frames ]   [ Frames ]    [%]
---- ---- --- ------ ----- ----------------- ----------------- ----------------- ------------ ------------ ------ ------
   1    1   7 G/1    Yes       50.000/49.023     49 .995/49.019       0 .000/0.000            0            0         FAIL
   1    1   7 Y/1    Yes                                               0.000/0.000            0            0         FAIL

Delay Measurements :
--- --- ------ ----- -------- -------- ----------------- ----------------- ------
UNI UNI Step  # Under UNI Ingr UNI Egr  Min  /Avg/Max        Min /Avg/Max        Status
Ing Egr        Test                      Delay             Delay Var    .
CoS CoS               [Frames] [Frames] [usecs]            [ usecs]
--- --- ------ ----- -------- -------- ----------------- ----------------- ------
  7   7      1  Yes         2        0                                      FAIL
```

Actually the test fails for more than that reason, but internally in the Y.1564 software, delay measurements are checked before test traffic, and only the first reason for a failing test is printed in the report.

If one looks at the UNI Ingr In-Service frame count, it is zero. That means that none of the frames that were applied were counted on the ECE under test. The reason for this is most likely an EVC/ECE configuration error: The traffic could be absorbed by another ECE than the one we attempt to hit. Remember that frames are matched against ECEs in the order they are added to hardware, and if the frames match another ECE that comes before the one under test, that one will absorb the frames. That other ECE could map to the same EVC as we are testing or to another. In the example above, it matches another EVC, because otherwise that other ECE would have been displayed in the report – even when not under test – because its counters would have been non-zero.

UNI Egress Frame Count is Zero

In the following example, the UNI Ingress In-service counters are indeed non-zero, but the UNI Egress counters are zero.

```
Status :
  Started at                  : 1970-01-03T23:50:29+00:00
  Ended at                    : 1970-01-03T23:50:30+00:00
  Status                      : Failed
  Details                     : Delay Measurements : Acceptable frame loss exceeded

Test Results :
---- ---- --- ------ ----- ----------------- ----------------- ----------------- ------------ ------------ ------ ------
UNI  UNI  UNI Color / Under UNI Ingr  (L1/L2)  UNI Ingr (L1/L2)  UNI Ingr (L1/L2)  UNI Ingr     UNI Egr      Frame  Status
Ingr Egr  Ing Step  # Test  Requested         Applied          In   -service       In -service                Loss
ECE  ECE  CoS             [Mbps]            [ Mbps ]           [ Mbps ]           [ Frames ]    [ Frames ]     [%]
---- ---- --- ------ ----- ----------------- ----------------- ----------------- ------------ ------------ ------ ------
   1    1   7 G/1    Yes       50.000/49.023     49.995/49.019     49.621/48.651         6239            0 100   .00 FAIL
   1    1   7 Y/1    Yes                                            0.000/0.000            0            0          PASS

Delay Measurements :
--- --- ------ ----- -------- -------- ----------------- ----------------- ------
UNI UNI Step  # Under UNI Ingr UNI Egr  Min  /Avg/Max       Min /Avg/Max       Status
Ing Egr       Test                      Delay             Delay Var    .
CoS CoS              [Frames ] [Frames] [usecs ]          [ usecs ]
--- --- ------ ----- -------- -------- ----------------- ----------------- ------
  7   7      1  Yes          2        0                                     FAIL
```

The test fails for the same reason as in the previous example, but the cause is another. The test frames were transmitted on NNI, but they were lost somewhere along the forwarding path.

To identify whether it is the remote or the local end that is configured incorrectly, a good starting point is the NNI port's port or EVC counters.

If you know that no other services are using the NNI port, look at the local end of NNI port counters, like this:

```
# Clear NNI port counters
clear statistics GigabitEthernet 1/2
# Re-run the test, possibly limiting the number of ECEs under test to one.
y1564 start my_report profile profile-OAM-unaware evc 10 ece 1
# Wait for the test to end
# ...

# Show NNI port counters
show interface GigabitEthernet 1/2 statistics

GigabitEthernet 1/2 Statistics:
Rx Packets:                             0   Tx Packets:                            6241
Rx Octets:                              0   Tx Octets:                          6289048
Rx Unicast:                             0   Tx Unicast:                            6241
Rx Multicast:                           0   Tx Multicast:                             0
Rx Broadcast:                           0   Tx Broadcast:                             0
Rx Pause:                               0   Tx Pause:                                 0

Rx 64:                                  0   Tx 64:                                    0
Rx 65-127:                              0   Tx 65-127:                                2
Rx 128-255:                             0   Tx 128-255:                               0
Rx 256-511:                         0   Tx 256-511:                         0
Rx 512-1023:                        0   Tx 512-1023:                     6239
Rx 1024-1526:                       0   Tx 1024-1526:                       0
Rx 1527-    :                       0   Tx 1527-    :                       0

Rx Priority 0:                      0   Tx Priority 0:                      0
Rx Priority 1:                      0   Tx Priority 1:                      0
Rx Priority 2:                      0   Tx Priority 2:                      0
Rx Priority 3:                      0   Tx Priority 3:                      0
Rx Priority 4:                      0   Tx Priority 4:                      0
Rx Priority 5:                      0   Tx Priority 5:                      0
Rx Priority 6:                      0   Tx Priority 6:                      0
Rx Priority 7:                      0   Tx Priority 7:                   6241

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 Jabbers:                         0
Rx Filtered:                        0
```

From this, you can see that 6241 frames are transmitted on NNI with priority 7. This corresponds to the 6239 test traffic frames plus the 2 DM frames. You can also see that no frames are received, so the problem must lie at the remote end.

Alternatively, you may use the EVC counters. Unfortunately, these counters get cleared when the Y.1564 test stops, so in order to utilize them, you must first prolong the CIR configuration test, and then look at the EVC counters on the fly.

```
# Temporarily shut down UNI port(s)
configure terminal
interface GigabitEthernet 1/3
shutdown

# Temporarily prolong the CIR configuration test to, say, 100 seconds
y1564 profile profile-OAM-unaware
cir-test duration 100 dm-interval 400 step-count 2
end

# Clear statistics on EVC #10
clear evc statistics 10

# Re-run the test, possibly limiting the number of ECEs under test to one.
y1564 start my_report profile profile-OAM-unaware evc 10 ece 1

# While the test is running, look at the EVC counters on the NNI port
show evc statistics 10 interface g 1/2
EVC ID 10, Interface GigabitEthernet 1/2 Statistics:

Rx Green Frames:                 0   Tx Green Frames:              59572
Rx Yellow Frames:                0   Tx Yellow Frames:                 0
Rx Red Frames:                   0
Rx Discard Frames:               0   Tx Discard Frames:                0
Rx Green Bytes:                  0   Tx Green Bytes:            60026956
Rx Yellow Bytes:                 0   Tx Yellow Bytes:                  0
Rx Red Bytes:                    0
Rx Discard Bytes:                0   Tx Discard Bytes:                 0

# Optionally stop the Y.1564 test
y1564 stop my_report

# Restore profile configuration and UNI port(s)
```

```
configure terminal
interface GigabitEthernet 1/3
no shutdown
y1564 profile profile-OAM-unaware
cir-test duration 1 dm-interval 300 step-count 2
end
```

Again, the test shows that frames indeed egress NNI, but don’t return. Similar checks can be done at the remote end.

Another useful trick is to see whether the remote end has learned the test traffic’s source MAC address in the MAC-table on the NNI port. For loops in the EVC domain, this requires that the EVC in the remote end is configured to have learning enabled.

For loops in the EVC domain the SMAC is learned on the EVC’s internal VLAN ID (1234 in our example).

For loops in the Port domain the SMAC is learned on the EVC’s VLAN ID (1000 in our example).

Here is an example of a snapshot of the remote end of MAC address table obtained right after a test has executed on a loop in the EVC domain:

```
# show mac address-table
Type   VID  MAC Address        Ports
Static 1   00:01:c1:00:b5:30  CPU
Static 1    33:33:00:00:00:01  GigabitEthernet 1/1-9 2.5GigabitEthernet 1/1 CPU
Static 1    33:33:00:00:00:02  GigabitEthernet 1/1-9 2.5GigabitEthernet 1/1 CPU
Static 1    33:33:ff:00:b5:30  GigabitEthernet 1/1-9 2.5GigabitEthernet 1/1 CPU
Dynamic 1  90:e2:ba:73:4d:d9  GigabitEthernet 1/1
Static 1    ff:ff:ff:ff:ff:ff  GigabitEthernet 1/1-9 2.5GigabitEthernet 1/1 CPU
Dynamic 1234 00:01:02:03:04:05  GigabitEthernet 1/2
Dynamic 1234 00:01:c1:00:00:03  GigabitEthernet 1/2
```

The two last entries are the two addresses used by the local end: 00:01:02:03:04:05 is the MAC address used by the simulated customer test traffic (set through Traffic SMAC in Y.1564 profile; *not available in all products*). 00:01:c1:00:00:03 is the SMAC of the UNI port used by the Y.1731 1DM frames.

Both SMACs are learned in VLAN ID 1234, which is the Internal VLAN ID, so in this case, the frames do indeed map to the correct EVC. If these two entries were missing, you should check the EVC and ECE configuration of the remote end and whether the NNI (and UNI) indeed are forwarding (not spanning tree discarding).

UNI Egress Traffic Counts in Unanticipated ECE

In the following example, the test fails because the looped frames are counting in another ECE than anticipated, while the delay measurements succeed.

```
Status :
  Started at                   : 1970-01-04T03:52:59+00:00
  Ended at                     : 1970-01-04T03:53:03+00:00
  Status                       : Failed
  Details                      : Test traffic : Acceptable frame loss exceeded

Test Results :
---- ---- --- ------ ----- -----------------  -----------------  -----------------  ------------  ------------  ------  ------
UNI  UNI  UNI Color / Under UNI Ingr  (L1/L2)  UNI Ingr  (L1/L2)  UNI Ingr  (L1/L2)  UNI Ingr      UNI Egr       Frame  Status
Ingr Egr  Ing Step  # Test  Requested         Applied           In   -service        In -service                  Loss
ECE  ECE  CoS               [Mbps]            [ Mbps]            [ Mbps]            [ Frames]     [ Frames]      [%]
---- ---- --- ------ ----- -----------------  -----------------  -----------------  ------------  ------------  ------  ------
   1    1   7 G/1    Yes        50.000/49.023     49.995/49.019     49.610/48.641          6601             0 100   .00 FAIL
   1    1   7 Y/1    Yes                                             0.000/0.000              0             0           PASS
   2    2   6 G/1    Yes                                             0.000/0.000              0         16441   0   .00 FAIL
   2    2   6 Y/1    Yes        38.247/37.500     37.756/37.019     37.425/36.694          4934             0 100   .00 PASS
   3    1   5 G/1    Yes        25.498/25.000     25.492/24.995     25.487/24.989          3298             0           FAIL
   3    1   5 Y/1    Yes                                             0.000/0.000              0             0           PASS
   4    2   4 G/1    Yes        12.750/12.500     12.484/12.240     12.496/12.250          1608             0           FAIL
   4    2   4 Y/1    Yes                                             0.000/0.000              0             0           PASS

Delay Measurements :
--- --- ------ ----- -------- -------- -----------------  -----------------  ------
UNI UNI Step  # Under UNI Ingr UNI Egr  Min  /Avg/Max       Min /Avg/Max       Status
Ing Egr       Test                      Delay              Delay Var    .
CoS CoS                [Frames] [Frames] [usecs]             [ usecs]
--- --- ------ ----- -------- -------- -----------------  -----------------  ------
  4   4      1  Yes         1        2         12  /12/12             0 /0/0 PASS
  5   4      1  Yes         1        0                                       PASS
  6   6      1  Yes         1        1         33  /33/33             0 /0/0 PASS
  7   7      1  Yes         1        1         12  /12/12             0 /0/0 PASS
```

The sum of all UNI ingress frames equals the UNI egress frame counter for ECE #2. This means that the looped traffic indeed contains the correct VLAN ID in the S-tag, but the PCP has been altered by the remote end. This typically means that the NNI port of the remote end of QoS ingress tag classification is not enabled or QoS egress port tag remarking is not set to mapped or the two maps are not identical (when ingress <PCP, DEI> maps to <CoS, DP>, the <CoS, DP> must map to the same <PCP, DEI> on egress).

This error is only possible when using simulated customer traffic as test traffic, since the S-tag's PCP value is not used when using Y.1731 as test traffic.

All Frames are Green on Return from Remote End

One of the frequently seen failures of the EIR configuration test is "`Received more green frames than were transmitted`".

In the following example, 6210 green frames and 1211 yellow frames were applied on ECE #3, but 7421 frames were returned as green (and counted on ECE #1, which is as expected with the example used).

```
Test Results :
---- ---- --- ------ ----- -----------------  -----------------  -----------------  ------------  ------------  ------  ------
UNI  UNI  UNI Color  Under UNI Ingr   (L1/L2)  UNI Ingr  (L1/L2)  UNI Ingr  (L1/L2)  UNI Ingr      UNI Egr       Frame  Status
Ingr Egr  Ing        Test  Requested         Applied           In    -service        In -service                  Loss
ECE  ECE  CoS               [Mbps]            [ Mbps]            [ Mbps]            [ Frames]     [ Frames]      [%]
---- ---- --- ------ ----- -----------------  -----------------  -----------------  ------------  ------------  ------  ------
   1    1   7 Green  Yes                                             0.000/0.000              0          7421   0   .00 SKIP
   1    1   7 Yellow Yes                                             0.000/0.000              0             0   0   .00 SKIP
   3    1   5 Green  Yes        50.996/50.000     50.954/49.959     50.872/49.878          6210             0           PASS
   3    1   5 Yellow Yes        10.199/10.000      10.157/9.959       9.920/9.726          1211             0           PASS
```

7421 happens to be the sum of 6210 and 1211, so all frames were returned, but the DEI bit of the S-tag was cleared along the forwarding path.

Re-coloring of a frame can happen at a dual leaky bucket policer or at places where QoS mapping is done. Since a dual leaky bucket policer cannot paint a yellow frame green, it is very likely that this error stems from QoS mapping. But is it the QoS mapping happening at the local end of NNI egress, the remote end of NNI ingress, the remote end of UNI egress, the remote end of UNI ingress, the remote end of NNI egress, or the local end of NNI ingress?

We can rule out the local end of NNI egress, because only ECEs that have `Egress Outer Tag`’s `DEI Mode` set to `Drop Precedence` can be tested. With this setting, the color of the frame after it has been policed goes directly into the DEI bit of the S-tag on NNI.

We can also rule out the local end of NNI ingress, because the test wouldn’t start if the QoS tag classification on NNI wasn’t set to map DEI directly to DP.

In this example, we can also rule out remote end of UNI egress and remote end of UNI ingress, because the traffic loop is a facility loop. If it was a terminal loop, those two settings would also have to be examined.

In general, the remote end of QoS Ingress Port Tag Classification must be enabled on NNI (and UNI for terminal loops) and a one-to-one DEI-to-DP translation must be enforced. Likewise, the remote end of QoS Egress Port Tag Remarking must be set to Mapped on NNI (and UNI for terminal loops) and a one-to-one DP-to-DEI translation must be enforced.

Partial Frame Loss

Continuing with the example in Example Used, page 21-30, suppose you have enabled traffic-test-loop 4 at the remote end (this requires deleting traffic-test-loop 2) and disabled traffic-test-loop 1.

Executing a Y.1564 test of ECE #1 with the `profile-OAM-unaware` profile yields results similar to the following:

```
**************************************************    CIR configuration test   **************************************************
 Configuration :
  Duration per step             : 1 second
  Delay meas . interval         : 400 msecs
  Step count                    : 2

Status :
  Started at                    : 1970 -01 -05T03 :12 :18+00 :00
  Ended at                      : 1970 -01 -05T03 :12 :21+00 :00
  Status                        : Failed
  Details                       : Delay Measurements  : Acceptable frame loss exceeded

Test Results :
---- ---- --- ------ ----- -----------------  -----------------  -----------------  ------------  ------------  ------  ------
UNI  UNI  UNI Color / Under UNI Ingr  (L1/L2)  UNI Ingr  (L1/L2)  UNI Ingr  (L1/L2)  UNI Ingr      UNI Egr       Frame  Status
Ingr Egr  Ing Step  # Test  Requested         Applied           In   -service        In -service                 Loss
ECE  ECE  CoS             [Mbps ]            [ Mbps ]           [ Mbps ]          [ Frames ]    [ Frames ]      [%]
---- ---- --- ------ ----- -----------------  -----------------  -----------------  ------------  ------------  ------  ------
   1    1   7  G/1    Yes        50.000/49.023      49 .995/49.019      49 .850/48.876          6207          1254  79   .79 FAIL
   1    1   7  Y/1    Yes                                              0.000/0.000             0          3109          PASS

Delay Measurements  :
--- --- ------  -----  --------  --------  -----------------  -----------------  ------
UNI UNI Step  # Under UNI Ingr UNI Egr  Min  /Avg/Max       Min /Avg/Max       Status
Ing Egr        Test                        Delay           Delay Var    .
CoS CoS               [Frames ] [Frames ] [usecs ]          [ usecs ]
--- --- ------  -----  --------  --------  -----------------  -----------------  ------
  7   7      1  Yes          1        0                                           FAIL
```

The test fails with the well-known “`Delay Measurements: Acceptable frame loss exceeded`”, but in this case, we did indeed get some green and some yellow test traffic frames back from the remote end, but the sum of the returned frames doesn’t add up to the number of frames applied at UNI ingress.

Knowing that we used a terminal MAC-loop in the EVC-domain helps solving the problem: All simulated customer frames are looped on UNI of the remote end of EVC, where they indeed go through the remote end of policer for ECE #1. Looking closer at policer #1 in the remote end of configuration shows the following:

```
evc policer 1 enable rate-type line cir 10000 cbs 10000 eir 25000 ebs 10000
```

Compare it to policer 1 of the local end:

```
evc policer 1 enable rate-type line cir 100000 cbs 10000 eir 25000 ebs 10000
```

Found the typo? The CIR is configured to 10000 kbps instead of 100000 kbps. This means that only 1/5 of the frames come through when applying 50 Mbps at local end of UNI Ingress.

Be aware that using this particular traffic-test-loop configuration REQUIRES the policers to be disabled, because the DM frames bypass the policer at the local end, but go through the policer at the remote end, and because both DM and test traffic undergo the same SAC check.

If you run this test a couple of times, you will notice that sometimes the DM frames indeed pass through the remote end of policer, in which case the test with fail with "`Test traffic: Acceptable frame loss exceeded`".

On products supporting a terminal MAC-loop in the Port-domain, the remote end of policers are also of importance, because the frames will loop on UNI and get re-classified to the EVC if present at the remote end.

UNI Egress Exceeds UNI Ingress Frame Count

Sometimes, especially on untagged EVCs, the remote end transmits additional traffic on the NNI port that gets classified to the untagged EVC when it arrives at the local end. There will therefore be excess green traffic on the EVC and the Y.1564 test will fail.

It is important that the remote end - no matter switch vendor – takes the EVC out of service while performing Y.1564 tests.

Summary

The following table summarizes the most common reasons for a failing Y.1564 test:

***Table 13* • Common Reasons for Y.1564 Test Failure**

Symptom	Possible Reasons
UNI Ingress in-service frame count is zero	This happens with simulated customer traffic when another ECE that comes before the ECE under test captures the traffic. That other ECE may or may not be part of the EVC under test.

Table 13 • **Common Reasons for Y.1564 Test Failure**

Symptom	**Possible Reasons**
UNI Egress in-service frame count is zero	When for DST, the OAM-aware option is selected, the possible reasons for the symptoms are: • The remote end of loop is not configured as an OAM-Loop. • The OAM-Loop is disabled. • Another loop captures the traffic before the OAM-Loop. • The Peer MAC address specified during Y.1564 test start is not the MAC address of the NNI port when the remote end loop is a facility loop or the UNI port when the remote end loop is a terminal loop. • The MEG-level specified in the Y.1564 profile doesn't correspond to the MEG-level of the loop. • The loop is not a subscriber loop. When for DST, the OAM-aware option is cleared, the possible reasons for the symptoms are: • The remote end of NNI port is not configured as a MAC-loop. • The MAC-loop is disabled.
	There is no link on the NNI that reaches the loop-configured DST. The Y.1564 software checks that there is link on at least one of the EVC's NNI ports, but if DST is reached through an NNI without link, this error will occur.
	The remote end of NNI port is spanning tree discarding. If terminal-looping: The remote end of UNI port is spanning tree discarding.
	The local end of NNI port that reaches the loop-configured DST is spanning tree discarding. The Y.1564 software checks that at least one of the EVC's NNI ports at the local end is not spanning tree discarding, and that the UNI ports used under test are not spanning tree discarding.

Table 13 • **Common Reasons for Y.1564 Test Failure**

Symptom	Possible Reasons

	The VLAN configuration of the remote end is incorrect.
	If using facility MAC-loops, a simple VLAN unaware NNI configuration will work with both tagged and untagged EVCs:
	The VLAN configuration of the remote end is incorrect.
	If using facility MAC-loops, a simple VLAN unaware NNI configuration will work with both tagged and untagged EVCs:
	`switchport access vlan 4095`
	`switchport hybrid native vlan 4095`
	`switchport hybrid allowed vlan none`
	`switchport hybrid port-type unaware`
	`switchport mode hybrid`
	If using terminal OAM-loops, both UNI and NNI must be configured properly. Here is an example for NNI:
	`switchport hybrid native vlan 4095`
	`switchport hybrid allowed vlan none`
	`switchport hybrid port-type s-port`
	`switchport mode hybrid`
	For UNI, omit the port-type s-port line.

	The QoS configuration of the remote end is incorrect. When using simulated customer traffic as test traffic, the PCP returned in the outer tag by the remote end must be the same as it ingressed remote end's NNI with. A QoS ingress tag classification on the remote end of NNI port that performs a one-to-one mapping of outer tag's <PCP, DEI> to <QoS, DP>, and vice versa for QoS egress mapping is recommended. For terminal loops, also the UNI should have this configuration.
UNI Egress counts in another ECE than anticipated	As above, make sure VLAN and QoS is configured correctly on the remote end.
All frames are green on return from remote end	This is normally a result of QoS Ingress Tag Classification and QoS Egress Tag Remarking enabled on remote end of NNI - and if terminal loop - on remote end's UNI. Additionally, there must be a one-to-one DEI-to-DP and DP-to-DEI translation.
UNI Egress exceeds UNI ingress	This could be a result of real subscriber traffic entering the EVC at the remote end’s UNI. If using a Cisco switch as remote end, the traffic test loop software makes sure to take the UNI port or EVC out of service, but a wrong configuration of the remote end may still result in traffic from other ports to egress remote end’s NNI and get classified to the EVC, causing the test to fail.

CHAPTER 22

Configuring LAG State

This document gives examples on how to configure LAG state using Industrial Command Line Interface (ICLI). The examples used in this document pertain to ENT switch products.

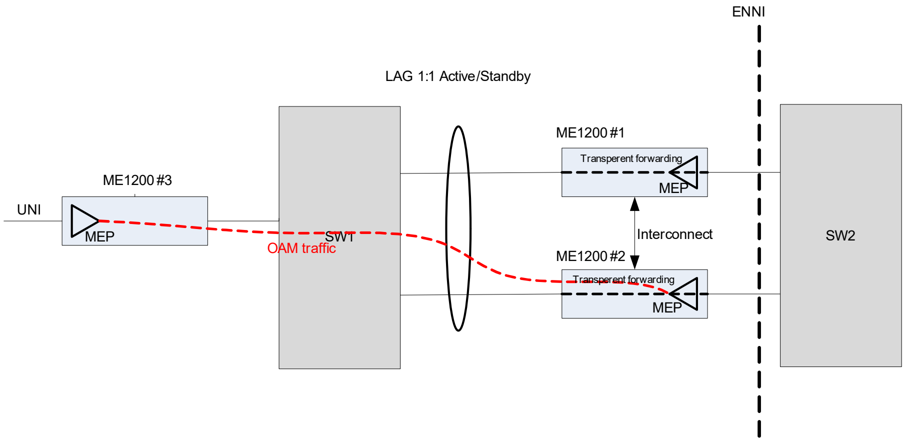
Audience

This document is for software and application developers who need to understand and use the LAG State functionality on the ENT switch products.

The LAG State application

The Application

Figure 22-1 **LAG state setup**



SW1 and SW2 conform a 1:1 LAG between them (using LACP), i.e. only one link is active at time. The other link is in standby mode and becomes active if the first one fails.

The 2 ME1200 NIDs (#1 and #2) between SW1 and SW2 in Figure 1, transparently forward all traffic , incl. BPDUs. In the process the LACP frames are snooped to determine the state of the LACP protocol before they are passed along. SW1 and SW2 are not aware of the ME1200's.

Inside ME1200 #1 and #2 the LAG state module is configured. The SW module passes the state of the LACP protocol to subscribers of this information. This could be the MEP module which will only become active the link is in Active state. Only one of the 2 ME1200s can have the state as active, i.e. only one of the MEP modules will be active at a time. When the MEP module is in Passive mode no OAM frames are transmitted and no OAM alarms are active, i.e. it's in "sleeping" mode.

The MEP modules in ME1200 #1 and #2 are identically configured. The MEP in ME1200 #3 is not aware of, if the peer MEP changes from #1 to #2 or vice versa.

Management

The 2 ME1200 are individually configured, i.e. single point of management (SPOM) in not supported. The configuration can be performed via ICLI, SNMP or Web.

Interconnect link

To ensure NID-NID coordination the partner NID is also updated if the state changes. If both NIDs have the same state then the NID with the lowest mac address will go into active mode while the other will go into passive mode. To avoid single point of failure the interconnect link can be statically aggregated. If the primary (configured) interconnect port goes down the lag state module will silently change to the other aggregated port for frame transmission. The id of the current interconnect -port in use can be viewed through ICLI.

Note that the LAG state functionality will work without an interconnect link even though this is not recommended. The LAG state will then only be based upon the state of the local LACP protocol.

MEP module

The MEP module receives callbacks when the state changes. The pass-through port-pair is included in the callback as well as the state. The MEP module will disable all MEP instances which uses either of the 2 ports. MEP instances not using one of the 2 ports are not touched.

Configuration Examples

The following section an example is given for how to configure the unit using the ICLI.

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

```
# reload defaults
```

Configuration through ICLI

To achieve the setup described in Figure 1, the following is performed on both the ME1200s (#1 and #2):

Gig 1/1 is connected to SW1, as pass-through port 1.

Gig 1/2 is connected to SW2, as pass-through port 2.

Gig 1/3 is connected to the other ME1200 as interconnect port.

```
# conf terminal
lag-state 1 port1 int Gi 1/1 port2 int Gi 1/2 interconnect int Gi 1/3
(config)#
```

Status through ICLI

To view the configuration and the status the following is issued on one of the ME1200s:

```
# show lag-state
Configuration:
Lag-state port 1      : Gi 1/1
Lag-state port 2      : Gi 1/2
Interconnect port     : Gi 1/3

Status (and time since update):
Last partner status   : PASSIVE     (00:00:00)
Last LACP status      : ACTIVE      (00:00:01)
Current status        : ACTIVE      (00:00:08)

LACP protocol state:
Lag-state port     Activit Timeout Aggrege Synchro Collect  Distrib  Default
    Expired
Gi 1/1            Active   Fast     Yes      Yes      Yes      Yes      No       No
Gi 1/2            Active   Fast     Yes      Yes      Yes      Yes      No       No
```

The configuration is displayed and then actual status.

“Partner status” is the last status seen from partner.

“LACP status” is the last status seen from the LACP protocol.

“Current status” is the state of the LAG link and what has been reported to subscribers.

The partner ME1200 should have an opposite “Current status”, i.e. PASSIVE in the above example.

The time since last update us also displayed.

The LACP protocol state is displayed as seen on each of the 2 ports.

MEP status

To verify that the MEP module has received the LAG state info the following is issued:

```
# show mep detail
MEP Basic Configuration is:
 Inst . . . .     MAC  LAG
   1  . . . .  00-01-C1-00-CB-41 ACTV
```

I.e. the state is Active.

Or

```
 Inst . . . .     MAC  LAG
   1  . . . .  00-01-C1-00-CB-41 STNB
```

I.e. the state is Standby.

Configuration of aggregated interconnect port

The interconnect port can be aggregated with another port to avoid a single point of failure. To aggregate interconnect port 3 with port 4 the following commands are is issued:

```
# conf terminal
# interface GigabitEthernet 1/3,4
(config-if)# aggregation group 1
# show lag-state
Configuration:
Lag-state port 1     : Gi 1/1
```

```
Lag-state port 2      : Gi 1/2
Interconnect port     : Gi 1/3

Status:
Last partner status   : PASSIVE
Last LACP status      : ACTIVE
Current status        : ACTIVE
Partner Rx/Tx port    : Gi 1/3 (aggr id 1)
```

Note that the aggregation id is displayed as a partner port. If Gig1/3 goes down then Gig 1/4 will take over and be displayed in the show status command.

Configuring Remote Login and Data Transfer

This document gives examples on how to configure FTP Client, Telnet client using Industrial Command Line Interface (ICLI) for connecting to remote Servers. The examples used in this document pertain to ENT switch products.

Audience

This document is for application developers and software engineers who need to understand and use the FTP Client or telnet client functionality on the ENT switch products.

References

Table 23-1 Configuration guide references

Document	Description
ENT-AN1104	ICLI Configuration Guide
RFC-959	File Transfer protocol RFC
RFC-854	Telnet protocol specification RFC

FTP Client

FTP Overview

FTP or File transfer protocol is used to transfer files between two network devices using Client Server architecture. An FTP Client tries to connect to Server presenting valid user credentials. After validating the user credentials, the FTP Client would request for file transfer between client and server.

FTP protocol has two modes of operation i.e. active and passive modes. By default, FTP Client connects in active mode to Server. But, some of the firewalls do not support FTP active mode of operation. To solve this issue, FTP passive mode of operation can be used.

There are two ports used by FTP protocol on both client and server. One is command port and other is data port. Command ports are used for exchanging FTP commands and data ports are used for transferring the actual data. FTP uses TCP connection for both command and data connection. In any mode, Client initiates command connection to Server. In Active FTP mode, Server initiates data connection to Client. But, some firewalls on Client systems have issues with Server initiating connection to Client. So, Passive FTP mode is used in such scenarios. In Passive FTP mode, Client initiates both command and data connections to the Server.

FTP can be used for different purposes involving file transfer. The primary usage of FTP protocol can be to download an image from server and upgrade the firmware. FTP can be used to download CLI configuration files on to the ENT switch and update the running configuration of the ENT switch. It can also be used to copy the starting configuration file on the ENT Switch to a remote Server. It can be used to copy any existing files on the ENT Switch to any remote FTP Server.

On the ENT Switches, files are stored on the flash. So, the location of the file on flash would be used for file transfer with remote Server. This will be useful for copying configuration files to and from the ENT Switch. The different scenarios related to using ftp client are mentioned in below sections.

FTP Client Configuration examples

The following sections describe FTP Client functionality in detail with examples on different scenarios on ENT Switch using ICLI commands.

Set the FTP mode of operation to Passive

By default, FTP Client tries to connect to Server in Active mode of operation. If the FTP Passive mode of operation is required, the corresponding ICLI command must be given on ENT Switch as shown below.

(config)# ip ftp client-mode passive

The execution of ICLI command for Passive FTP would ensure all subsequent FTP transfers from the Client are done in FTP Passive mode of operation. The above ICLI command should be executed before doing file transfer.

Unset the FTP Passive mode of operation to Active mode

If Passive mode of FTP is configured, then to change the FTP mode to Active, the corresponding ICLI command must be given on the ENT Switch as shown below.

```
(config)# no ip ftp client-mode passive
```

The execution of the above ICLI command would ensure that all subsequent FTP transfers from the Client are done in FTP Active mode of operation. The above ICLI command should be executed before doing file transfer.

Check the current running configuration of FTP Passive mode

FTP Passive mode configuration can be seen in the running configuration of ENT Switch. If there is no passive mode configuration seen in the ‘running-config’ of ENT Switch, then FTP Client connects to server in Active mode.

```
# show running-config
Building configuration...
username admin privilege 15 password none
ip ftp client-mode passive
!
vlan 1
!
!
ztp fallback vlan 1-4095 frame-type tagged interface Gi 1/1-9
ztp fallback vlan 1 frame-type untagged interface Gi 1/1-9

spanning-tree mst name 00-01-c1-00-f8-90 revision 0
!
interface GigabitEthernet 1/1
 lldp med type end-point
```

Firmware upgrade

To upgrade firmware using ftp when remote server contains the image, the equivalent ICLI command can be given as shown below. To connect to FTP Server in Passive mode, the equivalent FTP Passive mode ICLI command must be given before executing this operation.

```
# firmware upgrade ftp://user:password@10.1.1.1/image_name
Fetching...
looking up 10.1.1.1
connecting non-blocking to 10.1.1.1:21
connection: No error
binding data socket
initiating transfer
Waiting for firmware update to complete
Starting flash update - do not power off device!
Erasing image...
Programming image...
 ... Erase from 0x40ff0000-0x40ffffff: .
... Program from 0x87feeffc-0x87ffeffc to 0x40ff0000: .
... Program from 0x87fef006-0x87fef008 to 0x40ff000a: .
Flash update succeeded.
```

In the Sample ICLI command given above, the keywords 'user' and 'password' represent username and password credentials acceptable to remote server '10.1.1.1'. ‘image_name’ is the name of the image to be upgraded on the Switch. Image is downloaded using ftp protocol and then programmed on to the flash of ENT Switch.

Copy Startup Config to Remote Server

To copy startup-config from ENT Switch flash to remote server '10.1.1.1', the equivalent ICLI command can be given as below.

```
# copy startup-config ftp://user:password@10.1.1.1/startup.txt
% Saving 1142 bytes to 10.1.1.1 /startup.txt
looking up 10.1.1.1
```

```
connecting non-blocking to 10.1.1.1:21
connection: No error
binding data socket
initiating transfer
% FTP save SUCCESS for 1142 bytes
```

The file 'startup.txt' represent the destination name of the file on remote server '10.1.1.1'. To connect to FTP Server in Passive mode, the equivalent FTP Passive mode ICLI command must be given before executing this operation.

Copy file from ENT Switch to Remote Server

To copy the file ‘config.txt’ from ENT Switch flash to remote Server, check whether the file exists or not using ‘dir’ command as shown below. If it exists, the equivalent ICLI command can be given as below.

```
# dir
Directory of flash:
    r- 1970-01-01 00:00:00      412 default-config
    rw 1970-01-02 18:10:50     1142 startup-config
    rw 1970-01-01 00:25:02     1170 config.txt
3 files, 2724 bytes total.
#
# copy flash: config.txt ftp://root@10.1.1.1/temp.txt
% Saving 1170 bytes to 10.1.1.1 /temp.txt
looking up 10.1.1.1
connecting non-blocking to 10.1.1.1:21
connection: No error
binding data socket
initiating transfer
% FTP save SUCCESS for 1170 bytes
```

To connect to FTP Server in Passive mode, the equivalent FTP Passive mode ICLI command must be given before executing this operation.

Copy file from Remote Server to ENT Switch

To Copy file ‘temp.txt’ from remote Server to ENT Switch as ‘config.txt’, the equivalent ICLI command can be given as below.

```
# copy ftp://root@10.1.1.1/temp.txt flash: config.txt
looking up 10.1.1.1
connecting non-blocking to 10.1.1.1:21
connection: No error
binding data socket
initiating transfer
 FTP load SUCCESS
% Saving 1170 bytes to flash: config.txt
#
# dir
Directory of flash:
    r- 1970-01-01 00:00:00      412 default-config
    rw 1970-01-02 18:10:50     1142 startup-config
    rw 1970-01-01 00:13:06     1170 config.txt
3 files, 2724 bytes total.
```

The ICLI command ‘dir’ can be used to see all the files currently stored on the flash. To connect to FTP Server in Passive mode, the equivalent FTP Passive mode ICLI command must be given before executing this operation.

FTP Special cases

The maximum size of file that can be copied onto ENT Switch using ‘Copy’ command is limited to 4MB. The example given below shows the issue of oversize file.

```
# copy ftp://root@10.1.1.1/me1200-universal-serval-mz.img flash:config.txt
looking up 10.1.1.1
connecting non-blocking to 10.1.1.1:21
connection: No error
binding data socket
initiating transfer
% FILE too large than available buffer of 4194304 bytes
 FTP load FAILED
```

Firmware upgrade can download image which can be stored on the flash of corresponding ENT Switch. The maximum size of image allowed depends on the flash size of corresponding boards. For ME1200 ENT Switches, the maximum size of image allowed is around 6MB.

Telnet Client

Telnet overview

Telnet is an application layer protocol that runs over TCP/IP network to provide interactive communication with remote network devices. Users would interact with network devices through terminals. The telnet client would run on such network devices to establish connection with server. There would be a Telnet server listening for connections from Telnet client devices. Telnet clients would try to connect to server using its IP address and listening port. Once the connection is established, it would appear that user terminals are interacting directly with the server bypassing the network device with telnet client.

In general, Telnet servers listen on port 23. But, it is not mandatory to listen on port 23 only. A Telnet client would try to establish TCP connection to server. TCP is a reliable transport protocol which implies that Telnet data transfer would follow TCP mechanisms for preventing data loss. After connection establishment, Telnet clients would negotiate options with server. During option negotiation, both Telnet client and server would agree on the services supported by them. Option negotiation would be done using IAC (interpret as command) characters with Ascii value 255. Data following the IAC characters would be interpreted as Telnet commands having option information. RFC 854 describes some of the Telnet commands and their Ascii codes.

Once the option negotiation is done, the data typed by users at terminals would be received at Telnet client first. Telnet client would process the data for any escape sequence of characters. If no escape characters found, the data would be forwarded to server. Few character sequence is determined as escape sequence so that the Telnet client would use them as instructions to the Telnet client. When the Telnet client receives these character sequence, it would not forward those characters to server but use them to send corresponding Telnet commands to Server.

Whenever the Server receives any data from Telnet client and if server agrees on supporting ECHO option, it would echo the data back to client. After processing client data, it would send the result back to the client. The client would in turn send it to user terminal for displaying the data at terminal.

Note Telnet client on ME1200 switches expect the Server to echo the data back to client.

Telnet client configuration examples

The following sections describe how to configure telnet client on ENT switch with ICLI command examples.

Telnet access to server on default port 23

To access Telnet server on default port 23, the equivalent ICLI command can be given as below.

```
# telnet 10.9.61.203
Trying 10.9.61.203 ... Open

User Access Verification

Password:
me3600>en
Password:
me3600#
me3600#
```

Telnet access to server with IPv6 address

To access Telnet server with IPv6 address on default port, the equivalent ICLI command can be given as below.

```
# telnet 3000:1::1
Trying 3000:1::1 ... Open

User Access Verification
Password:
me3600>en
Password:
me3600#
```

Telnet access to server with hostname

To access Telnet server with hostname, the equivalent ICLI command can be given as shown below.

```
# telnet XXXENT0001.xx.net
Trying XXXENT0001.xx.net ... Open
==============================================================
  .\scripts\allusers.bat
  this script is executed for all users
  delete/rename it if you dont need it
 ==============================================================
Active code page: 437
C:\Users\XXX>
C:\Users\XXX.>
```

Telnet access to server running on specific port

To access Telnet server running on specific port, the equivalent ICLI command can be given on ENT switch as shown below.

```
# telnet 10.9.61.64 2323
Trying 10.9.61.64, 2323 ... Open

Username: admin
Password:
#
```

Send AYT (Are You There?) command to Server

To send Telnet AYT command from telnet client to server, the Keyboard sequence (Ctrl + ^ + T) must be pressed at terminal. The Telnet client would send a AYT command to Server. The response from server would be specific to that particular server.

```
# telnet 10.9.61.13 2015
Trying 10.9.61.13, 2015 ... Open

Username: admin
Password:
#
[Yes]  — After pressing (Ctrl + ^ + T)
#
```

Display help for escape characters

To display help for Telnet escape character sequence, the keyboard sequence (Ctrl + ^ + ?) must be pressed at terminal. The Telnet client would send the escape sequence to user terminals.

```
# telnet 10.9.61.64 2323
Trying 10.9.61.64, 2323 ... Open

Username: admin
Password:

[Special telnet escape help] — After pressing (Ctrl + ^ + ?)
  ^^B Send Telnet BREAK
  ^^T Send Telnet AYT
```

Send Break command to Server

To send Telnet Break command from telnet client to server, the Keyboard sequence (Ctrl + ^ + B) must be pressed at terminal. The Telnet client would send Break command to Server. The response from server would depend on that particular server.

```
# telnet 10.9.61.13 2015
Trying 10.9.61.13, 2015 ... Open
#            → Server hung for one keystroke after sending break command here
```

Disconnect Telnet session

To disconnect telnet session, the keyboard sequence (Ctrl + ^ + X) must be pressed at terminal. The Telnet client would disconnect the session with Telnet server and the user session on ME1200 switch would be resumed.

```
# telnet 10.9.61.64 2323
Trying 10.9.61.64, 2323 ... Open

Username: admin
Password:
#
 ..... Closing .....—After pressing (Ctrl + ^ + X) keyboard sequence
```

CHAPTER 24

Archive Logger

This document provides examples on how to configure and use configuration archive logger using the Industrial Command Line Interface (ICLI). The examples used in this document pertain to ENT switch products.

Overview of Archive Logger Configuration

The configuration archive logger allows the tracking of all configuration changes done by specific user in a particular session. The size or the number of entries in the configuration archive log can be configured from the CLI. At any instance of time, there can be maximum 1000 entries in the configuration archive log. The default number of entries in the configuration archive log is 100.

Each CLI command, supporting configuration change, is logged into configuration logger along with other attributes such as index, session id, username, and command line terminal used. Each entry or record in the configuration log is uniquely identified by an index. Each session is uniquely identified from the time the CLI mode enters global configuration mode till the time CLI mode exits it. Username identifies the user who entered the CLI commands. The tab space added before any command is an indication of the configuration mode level above global configuration mode. It is also added in case of exit from the current mode level.

The configuration archive logger supports configuration changes done through CLI only.

Archive Logging Configuration Examples

The following examples describe how to configure and use the configuration archive logging feature.

Enable the Archive Logging

The archive logging is enabled using the following set of commands.

```
# conf terminal
(config)# archive
(config-archive)# log config
(config-archive-log-cfg)# logging enable
(config-archive-log-cfg)#
```

Once it is done, each CLI command entered in any configuration mode is logged into the archive log.

Configure the Size of Archive Log

The default size of archive log is 100. It can be modified to any value up to 1000 using the following CLI commands. If the current size of the archive log is greater than configured size, the existing archive log is trimmed to configured size such that oldest entries are removed first.

```
(config)# archive
(config-archive)# log config
(config-archive-log-cfg)# logging size 30
(config-archive-log-cfg)#
```

Retrieve the Current Configuration of Archive Logging

The existing `show running-config` command displays the current running configuration of archive logging feature. The following configuration is one such example.

```
# show running-config
Building configuration...
username admin privilege 15 password none
evc 1 vid 100 ivid 100 interface GigabitEthernet 1/1
evc 2 vid 100 ivid 100 interface GigabitEthernet 1/2
evc ece 1 interface GigabitEthernet 1/3 cos 0
evc ece 2 interface GigabitEthernet 1/4 cos 0
!
archive
 log config
  logging enable
  logging size 30
!
vlan 1,2,10,11
!
!
!
#
```

Disable Archive Logging

Archive logging can be disabled using the following commands.

```
# conf t
(config)#
(config)# archive
(config-archive)# log config
(config-archive-log-cfg)# no logging enable
(config-archive-log-cfg)#
```

Configure the Archive Log Size to Default Value

The size of archive log is set to default value of 100 using the following commands. If the existing size is greater than default size, then the oldest entries are deleted till the existing size is equal to configured value.

```
(config)# archive
(config-archive)# log config
(config-archive-log-cfg)# no logging size
(config-archive-log-cfg)#
```

Retrive the Entire Contents of Archive Log

The following command displays the contents of the archive log.

```
(config)# archive
(config-archive)# log config
(config-archive-log-cfg)# logging enable
(config-archive-log-cfg)# exit
(config-archive)# exit
(config)# interface GigabitEthernet 1/4
(config-if)# shutdown
(config-if)# no shutdown
(config-if)# exit
(config)# exit
#
#
# show archive log config all
 idx   sess    user@line      Logged command
  1     1     admin@console   | exit
  2     1     admin@console   |  exit
  3     1     admin@console   |interface GigabitEthernet 1/4
  4     1     admin@console   | shutdown
  5     1     admin@console   | no shutdown
  6     1     admin@console   | exit

#
```

Retrieve the Contents of Archive Log Based on Log Entry Indices

The following command displays the archive log entries using specific index values.

```
# show archive log config 2 5
 idx   sess     user@line      Logged command
  2     1      admin@console   |   exit
  3     1      admin@console   |interface GigabitEthernet 1/4
  4     1      admin@console   | shutdown
  5     1      admin@console   | no shutdown
```

Retrieve User and Session index Specific Contents of Archive Log

The following example displays the archive log contents logged by specific user in a particular session.

```
# show archive log config user abcd session 3
 idx   sess   user@line     Logged command
  7     3     abcd@vty1     |interface vlan 1
  8     3     abcd@vty1     | ip address dhcp
  9     3     abcd@vty1     | exit

#
```

Clear the Archive Log Contents

The following example displays how to clear the contents of the archive log.

```
# show archive log config all
 idx   sess   user@line       Logged command
  1     1    admin@console    |  exit
  2     1    admin@console    |   exit
  3     1    admin@console    |interface GigabitEthernet 1/4
  4     1    admin@console    | shutdown
  5     1    admin@console    | no shutdown
  6     1    admin@console    | exit
  7     3     abcd@vty1       |interface vlan 1
  8     3     abcd@vty1       | ip address dhcp
  9     3     abcd@vty1       | exit

# clear archive log config
This will delete all entries in the config log buffer.
Enter Y if you are sure you want to proceed. ? [no]: Y
#
# show archive log config all
 idx   sess           user@line      Logged command
```

Enable SYSLOG Notification

The following example shows how to enable Syslog notification for configuration changes. It must be noted that Syslog notification is sent only when the archive logging is enabled. To disable the Syslog notification, the `no` form of the command can be used.

```
(config)# archive
(config-archive)# log config
(config-archive-log-cfg)# notify syslog
(config-archive-log-cfg)#
```