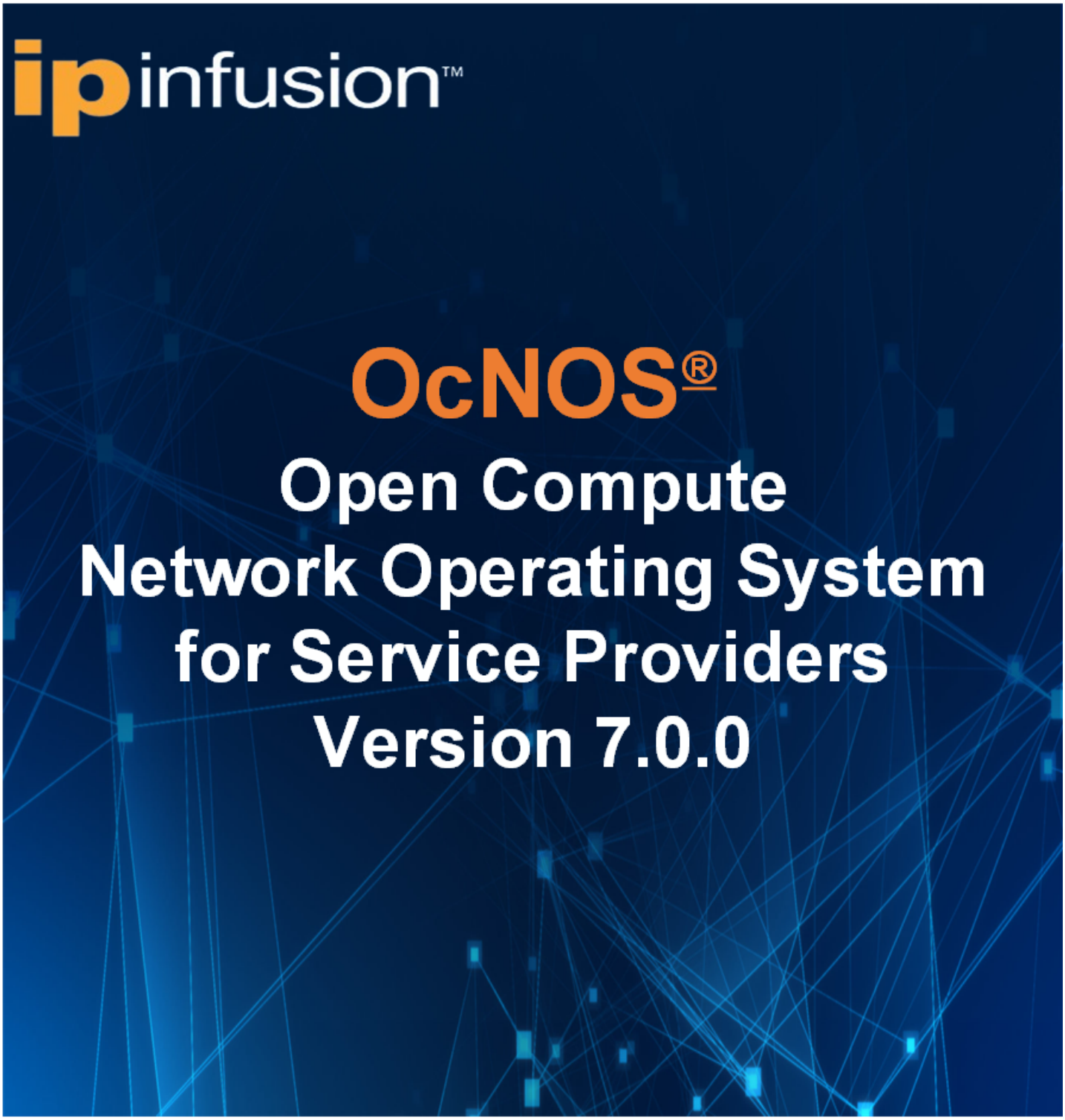


Layer 2 Guide

February 2026

IP Infusion Inc.

3979 Freedom Circle

Suite 900

Santa Clara, California 95054

http://www.ipinfusion.com/

For support, questions, or comments via E-mail, contact:

support@ipinfusion.com

Contents

Preface

This guide describes how to configure OcNOS.

Audience

This guide is intended for network administrators and other engineering professionals who configure OcNOS.

Conventions

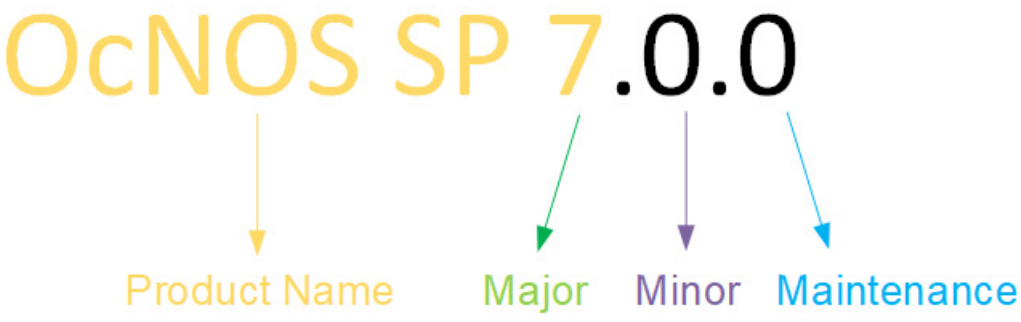
Table 1 on page 14 shows the conventions used in this guide.

Table 1: Conventions

Convention	Description
Italics	Emphasized terms or titles of books
Note:	Special instructions, suggestions, or warnings
`monospaced type`	Code elements such as commands, parameters, files, and directories

IP Infusion Product Release Version

Each integer in release number indicates Major, Minor, and Maintenance release versions. Build numbers that follow the release numbers are for internal tracking and verification of the software build process and are visible to customers as part of the software version number.



Product Name: IP Infusion Product Family

Major Version: New customer-facing functionality that represents a significant change to the code base; including, a significant marketing change or direction in the product.

Minor Version: Enhancements or extensions to existing features, changes to address external needs, or internal ements might be motivated by improvements to satisfy new sales regions or marketing initiatives.

Maintenance Version: A collection of product bugs or hotfixes usually scheduled every 30 or 60 days, based on the number of hotfixes.

Related Documentation

For information about installing OcNOS, see the *Installation Guide* for your platform.

Feature Availability

Each OcNOS SKU contains a set of supported features. For a list of available features based on the SKU that you purchased. Refer to the *Feature Matrix*.

Migration Guide

Check the *Migration Guide* for necessary configuration changes before migrating from one version of OcNOS to another.

IP Maestro Support

Monitor devices running OcNOS Release 6.3.4-70 and above using IP Maestro software.

Technical Support

IP Infusion maintains an online technical support site that provides a variety of technical support programs for licensed OcNOS customers at the Technical Assistance Center.

Customers and partners enjoy full access to the support website. The site allows customers and partners to open technical support calls, update open calls with new information, and review the status of open or closed calls. The password-protected site includes technical documentation, Release Notes, and descriptions of service offerings.

Technical Sales

Contact the IP Infusion sales representative for more information about the OcNOS solution.

Technical Documentation

For core commands and configuration procedures, visit: Product Documentation.

For training videos, visit: OcNOS Free Training Videos.

For a list of supported platforms and SKUs of OcNOS features, refer to the OcNOS Feature Matrix.

Disclaimer

The global documentation site is evolving to provide an enhanced website user experience for select topics included in this release. Some guides are now available outside the existing documentation library and can be accessed directly from custom documentation landing pages. These guides offer robust in-built search functionality.

For the latest documentation, visit the product-specific documentation landing page and select the relevant guide.

Comments

If you have comments, or need to report a problem with the content, contact techpubs@ipinfusion.com.

Command Line Interface

This chapter introduces the OcNOS Command Line Interface (CLI) and how to use its features.

Overview

You use the CLI to configure, monitor, and maintain OcNOS devices. The CLI is text-based and each command is usually associated with a specific task.

You can give the commands described in this manual locally from the console of a device running OcNOS or remotely from a terminal emulator such as `putty` or `xterm`. You can also use the commands in scripts to automate configuration tasks.

Chapter Organization

The chapters in command references are organized as described in Command Description Format.

The chapters in configuration guides are organized into these major sections:

- An overview that explains a configuration in words
- Topology with a diagram that shows the devices and connections used in the configuration
- Configuration steps in a table for each device where the left-hand side shows the commands you enter and the right-hand side explains the actions that the commands perform
- Validation which shows commands and their output that verify the configuration

Command Line Interface Help

You access the CLI help by entering a full or partial command string and a question mark “?”. The CLI displays the command keywords or parameters along with a short description. For example, at the CLI command prompt, type:

```
> show ?
```

The CLI displays this keyword list with short descriptions for each keyword:

```
show ?
  application-priority          Application Priority
  arp                           Internet Protocol (IP)
  bfd                           Bidirectional Forwarding Detection (BFD)
  bgp                           Border Gateway Protocol (BGP)
  bi-lsp                        Bi-directional lsp status and configuration
  bridge                        Bridge group commands
  ce-vlan                       COS Preservation for Customer Edge VLAN
  class-map                     Class map entry
  cli                           Show CLI tree of current mode
  clns                          Connectionless-Mode Network Service (CLNS)
  control-adjacency             Control Adjacency status and configuration
  control-channel               Control Channel status and configuration
  cspf                          CSPF Information
  customer                      Display Customer spanning-tree
  cvlan                         Display CVLAN information
  debugging                     Debugging functions
```

```
  etherchannel                    LACP etherchannel
  ethernet                        Layer-2
...
```

If you type the ? in the middle of a keyword, the CLI displays help for that keyword only.

```
> show de?
debugging  Debugging functions
```

If you type the ? in the middle of a keyword, but the incomplete keyword matches several other keywords, OcNOS displays help for all matching keywords.

```
> show i? (CLI does not display the question mark).
interface  Interface status and configuration
ip         IP information
isis       ISIS information
```

Command Completion

The CLI can complete the spelling of a command or a parameter. Begin typing the command or parameter and then press the tab key. For example, at the CLI command prompt type `sh`:

```
> sh
```

Press the tab key. The CLI displays:

```
> show
```

If the spelling of a command or parameter is ambiguous, the CLI displays the choices that match the abbreviation. Type `show i` and press the tab key. The CLI displays:

```
> show i
  interface  ip         ipv6       isis
> show i
```

The CLI displays the `interface` and `ip` keywords. Type `n` to select `interface` and press the tab key. The CLI displays:

```
> show in
> show interface
```

Type ? and the CLI displays the list of parameters for the `show interface` command.

```
> show interface
  IFNAME  Interface name
  |       Output modifiers
  >       Output redirection
  <cr>
```

The CLI displays the only parameter associated with this command, the `IFNAME` parameter.

Command Abbreviations

The CLI accepts abbreviations that uniquely identify a keyword in commands. For example:

```
> sh int xe0
```

is an abbreviation for:

```
> show interface xe0
```

Command Line Errors

Any unknown spelling causes the CLI to display the error `Unrecognized command` in response to the ?. The CLI displays the command again as last entered.

```
> show dd?
% Unrecognized command
> show dd
```

When you press the Enter key after typing an invalid command, the CLI displays:

```
(config)#router ospf here
                        ^
% Invalid input detected at '^' marker.
```

where the ^ points to the first character in error in the command.

If a command is incomplete, the CLI displays the following message:

```
> show
% Incomplete command.
```

Some commands are too long for the display line and can wrap mid-parameter or mid-keyword, as shown below. This does *not* cause an error and the command performs as expected:

```
area 10.10.0.18 virtual-link 10.10.0.19 authent
ication-key 57393
```

Command Negation

Many commands have a `no` form that resets a feature to its default value or disables the feature. For example:

- The `ip address` command assigns an IPv4 address to an interface
- The `no ip address` command removes an IPv4 address from an interface

Syntax Conventions

Table 2 on page 19 describes the conventions used to represent command syntax in this reference.

Table 2: Syntax conventions

Convention	Description	Example
`monospaced font`	Command strings entered on a command line	`show ip ospf`
`lowercase`	Keywords that you enter exactly as shown in the command syntax.	`show ip ospf`
`UPPERCASE`	See Variable Placeholders	`IFNAME`
`()`	Optional parameters, from which you must select one. Vertical bars delimit the selections. Do not enter the parentheses or vertical bars as part of the command.	`(A.B.C.D|<0-4294967295>)`

Table 2: Syntax conventions (Continued)

Convention	Description	Example
`()`	Optional parameters, from which you select one or none. Vertical bars delimit the selections. Do not enter the parentheses or vertical bars as part of the command.	`(A.B.C.D|<0-4294967295>|)`
`()`	Optional parameter which you can specify or omit. Do not enter the parentheses or vertical bar as part of the command.	`(IFNAME|)`
`{}`	Optional parameters, from which you must select one or more. Vertical bars delimit the selections. Do not enter the braces or vertical bars as part of the command.	`{intra-area <1-255>|inter-area <1-255>|external <1-255>}`
`[]`	Optional parameters, from which you select zero or more. Vertical bars delimit the selections. Do not enter the brackets or vertical bars as part of the command.	`[<1-65535>|AA:NN|internet|local-AS|no-advertise|no-export]`
`?`	Nonrepeatable parameter. The parameter that follows a question mark can only appear once in a command string. Do not enter the question mark as part of the command.	`?route-map WORD`
`.`	Repeatable parameter. The parameter that follows a period can be repeated more than once. Do not enter the period as part of the command.	`set as-path prepend .<1-65535>`

Variable Placeholders

Table 3 on page 20 shows the tokens used in command syntax use to represent variables for which you supply a value.

Table 3: Variable placeholders

Token	Description
`WORD`	A contiguous text string (excluding spaces)
`LINE`	A text string, including spaces; no other parameters can follow this parameter
`IFNAME`	Interface name whose format varies depending on the platform; examples are: `eth0`, `Ethernet0`, `ethernet0`, `xe0`
`A.B.C.D`	IPv4 address
`A.B.C.D/M`	IPv4 address and mask/prefix
`X:X::X:X`	IPv6 address
`X:X::X:X/M`	IPv6 address and mask/prefix
`HH:MM:SS`	Time format

Table 3: Variable placeholders

Token	Description
`AA:NN`	BGP community value
`XX:XX:XX:XX:XX:XX`	MAC address

`<1-5>`
`<1-65535>`
`<0-2147483647>`
`<0-4294967295>`
	Numeric range

Command Description Format

Table 4 on page 21 explains the sections used to describe each command in this reference.

Table 4: Command descriptions

Section	Description
Command Name	The name of the command, followed by what the command does and when should it be used
Command Syntax	The syntax of the command
Parameters	Parameters and options for the command
Default	The state before the command is executed
Command Mode	The mode in which the command runs; see Command Modes
Applicability	The command introduced in a specific release version and modified or updated in subsequent versions.
Example	An example of the command being executed

Keyboard Operations

Table 5 on page 21 lists the operations you can perform from the keyboard.

Table 5: Keyboard operations

Key combination	Operation
Left arrow or Ctrl+b	Moves one character to the left. When a command extends beyond a single line, you can press left arrow or Ctrl+b repeatedly to scroll toward the beginning of the line, or you can press Ctrl+a to go directly to the beginning of the line.
Right arrow or Ctrl-f	Moves one character to the right. When a command extends beyond a single line, you can press right arrow or Ctrl+f repeatedly to scroll toward the end of the line, or you can press Ctrl+e to go directly to the end of the line.

Table 5: Keyboard operations (Continued)

Key combination	Operation
Esc, b	Moves back one word
Esc, f	Moves forward one word
Ctrl+e	Moves to end of the line
Ctrl+a	Moves to the beginning of the line
Ctrl+u	Deletes the line
Ctrl+w	Deletes from the cursor to the previous whitespace
Alt+d	Deletes the current word
Ctrl+k	Deletes from the cursor to the end of line
Ctrl+y	Pastes text previously deleted with Ctrl+k, Alt+d, Ctrl+w, or Ctrl+u at the cursor
Ctrl+t	Transposes the current character with the previous character
Ctrl+c	Ignores the current line and redisplays the command prompt
Ctrl+z	Ends configuration mode and returns to exec mode
Ctrl+l	Clears the screen
Up Arrow or Ctrl+p	Scroll backward through command history
Down Arrow or Ctrl+n	Scroll forward through command history

Show Command Modifiers

You can use two tokens to modify the output of a `show` command. Enter a question mark to display these tokens:

```
# show users ?
  | Output modifiers
  > Output redirection
```

You can type the | (vertical bar character) to use output modifiers. For example:

```
> show rsvp | ?
  begin     Begin with the line that matches
  exclude   Exclude lines that match
  include   Include lines that match
  last      Last few lines
  redirect  Redirect output
```

Begin Modifier

The `begin` modifier displays the output beginning with the first line that contains the input string (everything typed after the `begin` keyword). For example:

```
# show running-config | begin xe1
```

```
...skipping
interface xe1
 ipv6 address fe80::204:75ff:fee6:5393/64
!
interface xe2
 ipv6 address fe80::20d:56ff:fe96:725a/64
!
line con 0
 login
!
end
```

You can specify a regular expression after the `begin` keyword, This example begins the output at a line with either “xe2” or “xe4”:

```
# show running-config | begin xe[2-4]

...skipping
interface xe2
 shutdown
!
interface xe4
 shutdown
!
interface svlan0.1
 no shutdown
!
route-map myroute permit 2
!
route-map mymap1 permit 10
!
route-map rmap1 permit 2
!
line con 0
 login
line vty 0 4
 login
!
end
```

Include Modifier

The `include` modifier includes only those lines of output that contain the input string. In the output below, all lines containing the word “input” are included:

```
# show interface xe1 | include input
    input packets 80434552, bytes 2147483647, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 1, missed 0
```

You can specify a regular expression after the `include` keyword. This examples includes all lines with “input” or “output”:

```
#show interface xe0 | include (in|out)put
    input packets 597058, bytes 338081476, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 613147, bytes 126055987, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
```

Exclude Modifier

The `exclude` modifier excludes all lines of output that contain the input string. In the following output example, all lines containing the word “input” are excluded:

```
# show interface xe1 | exclude input
Interface xe1
  Scope: both
  Hardware is Ethernet, address is 0004.75e6.5393
  index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Administrative Group(s): None
  DSTE Bandwidth Constraint Mode is MAM
  inet6 fe80::204:75ff:fee6:5393/64
    output packets 4438, bytes 394940, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

You can specify a regular expression after the `exclude` keyword. This example excludes lines with “output” or “input”:

```
# show interface xe0 | exclude (in|out)put
Interface xe0
  Scope: both
  Hardware is Ethernet  Current HW addr: 001b.2139.6c4a
  Physical:001b.2139.6c4a  Logical:(not set)
  index 2 metric 1 mtu 1500 duplex-full arp ageing timeout 3000
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Bandwidth 100m
  DHCP client is disabled.
  inet 10.1.2.173/24 broadcast 10.1.2.255
  VRRP Master of :  VRRP is not configured on this interface.
  inet6 fe80::21b:21ff:fe39:6c4a/64
    collisions 0
```

Redirect Modifier

The `redirect` modifier writes the output into a file. The output is not displayed.

```
# show cli history | redirect /var/frame.txt
```

The output redirection token (>) does the same thing:

```
# show cli history >/var/frame.txt
```

Last Modifier

The `last` modifier displays the output of last few number of lines (As per the user input). The last number ranges from 1 to 9999.

For example:

```
#show running-config | last 10
```

String Parameters

The restrictions in Table 6 on page 25 apply for all string parameters used in OcNOS commands, unless some other restrictions are noted for a particular command.

Table 6: String parameter restrictions

Restriction	Description
Input length	1965 characters or less
Restricted special characters	“?”, “,”, “>”, “|”, and “=” The “|” character is allowed only for the `description` command in interface mode.

Command Modes

Commands are grouped into modes arranged in a hierarchy. Each mode has its own set of commands. Table P-7 lists the command modes common to all protocols.

Table 7: Common command modes

Name	Description
Executive mode	Also called *view* mode, this is the first mode to appear after you start the CLI. It is a base mode from where you can perform basic commands such as `show`, `exit`, `quit`, `help`, and `enable`.
Privileged executive mode	Also called *enable* mode, in this mode you can run additional basic commands such as `debug`, `write`, and `show`.
Configure mode	Also called *configure terminal* mode, in this mode you can run configuration commands and go into other modes such as interface, router, route map, key chain, and address family. Configure mode is single user. Only one user at a time can be in configure mode.
Interface mode	In this mode you can configure protocol-specific settings for a particular interface. Any setting you configure in this mode overrides a setting configured in router mode.
Router mode	This mode is used to configure router-specific settings for a protocol such as BGP or OSPF.

Command Mode Tree

The diagram below shows the common command mode hierarchy.

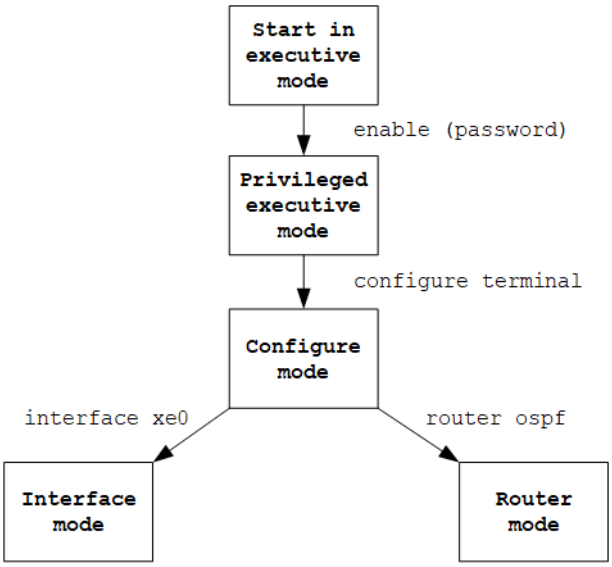


Figure 1: Common command modes

To change modes:

1. Enter privileged executive mode by entering `enable` in Executive mode.
2. Enter configure mode by entering `configure terminal` in Privileged Executive mode.

The example below shows moving from executive mode to privileged executive mode to configure mode and finally to router mode:

```
> enable mypassword
# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)# router ospf
(config-router)#
```

Note: Each protocol can have modes in addition to the common command modes. See the command reference for the respective protocol for details.

Transaction-based Command-line Interface

The OcNOS command line interface is transaction based:

- Any changes done in configure mode are stored in a separate *candidate* configuration that you can view with the `show transaction current` command.
- When a configuration is complete, apply the candidate configuration to the running configuration with the `commit` command.
- If a `commit` fails, no configuration is applied as the entire transaction is considered failed. You can continue to change the candidate configuration and then retry the `commit`.
- Discard the candidate configuration with the `abort transaction` command.
- Check the last aborted transaction with the `show transaction last-aborted` command.
- Multiple configurations cannot be removed with a single `commit`. You must remove each configuration followed by a `commit`.

Note: All commands MUST be executed only in the default CML shell (`cmlsh`). If you log in as root and start `imish`, then the system configurations will go out of sync. The `imish` shell is not supported and should not be started manually.

Layer 2 Configuration Guide

CHAPTER 1 Link Layer Discovery Protocol Configuration

This chapter contains a complete sample Link Layer Discovery Protocol (LLDP) configuration.

LLDP is a neighbor discovery protocol that defines a method for network access devices using Ethernet connectivity to advertise themselves to other devices on the same physical LAN, and then to store information about the network. It allows a device to learn higher-layer management reachability and connection endpoint information from adjacent devices. Using LLDP, a network device is able to advertise its identity, its capabilities and its media-specific configuration, as well as learn the same information from other connected devices.

Note: The `lldp-agent` command is not supported for SVLAN, VLAN, and loop-back interfaces.

Topology

Figure 1-1 displays a sample LLDP topology.

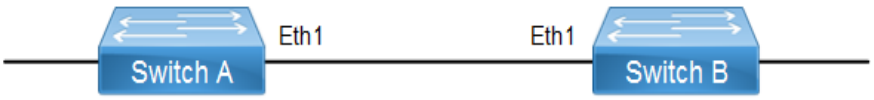


Figure 1-1: LLDP Topology

Interface Mode TLV

Default Agent

All configuration commands in the table below should be followed for each switch.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent`	Enter into the default agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#set lldp chassis-id-tlv ip-address`	Configure the subtype for chassis-id TLV
`(if-lldp-agent)#set lldp port-id-tlv mac-address`	Configure the subtype for port-id TLV
`(if-lldp-agent)#lldp tlv basic-mgmt port-description select`	Enable the `port-description TLV` to be transmitted on the port

`(if-lldp-agent)#lldp tlv basic-mgmt system-name select`	Enable the `system-name TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt system-capabilities select`	Enable the `system-capabilities TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt system-description select`	Enable the `system-description TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt management-address select`	Enable the `management-address TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-vlanid select`	Enable the `VLAN-id TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vlan-name select`	Enable the `VLAN-NAME TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-ptcl-vlanid select`	Enable the `Port and Protocol VLAN id TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific ptcl-identity select`	Enable the `Protocol Identity TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vid-digest select`	Enable the `VID Usage Digest TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific mgmt-vid select`	Enable the `Management VID TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific link-agg select`	Enable the `Link Aggregation TLV` to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific mac-phy select`	Enable the MAC/PHY Configuration/Status TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific max-mtu-size select`	Enable the Maximum Frame Size TLV to be transmitted on the port
`(if-lldp-agent)#set lldp timer msg-fast-tx 5`	Defines the time interval during fast transmission periods
`(if-lldp-agent)#set lldp tx-fast-init 6`	Defines the number of LLDPDUs that are transmitted during a fast transmission period
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#commit`	Commit the candidate configuration to the running configuration.
`(config-if)#exit`	Exit interface mode.

Validation

1. Verify the LLDP configurations in the local switch

```
#show running-config lldp
!
interface eth1
lldp-agent
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
  set lldp port-id-tlv mac-address
  lldp tlv basic-mgmt port-description select
  lldp tlv basic-mgmt system-name select
  lldp tlv basic-mgmt system-description select
  lldp tlv basic-mgmt system-capabilities select
  lldp tlv basic-mgmt management-address select
  lldp tlv ieee-8021-org-specific port-vlanid select
```

```
  lldp tlv ieee-8021-org-specific port-ptcl-vlanid select
  lldp tlv ieee-8021-org-specific vlan-name select
  lldp tlv ieee-8021-org-specific ptcl-identity select
  lldp tlv ieee-8021-org-specific vid-digest select
  lldp tlv ieee-8021-org-specific mgmt-vid select
  lldp tlv ieee-8021-org-specific link-agg select
  lldp tlv ieee-8023-org-specific mac-phy select
  lldp tlv ieee-8023-org-specific max-mtu-size select
  set lldp timer msg-fast-tx 5
  set lldp tx-fast-init 6
!
```

2. Verify the LLDP port statistics

```
#show lldp interface eth1 nearest-bridge

Agent Mode                    : Nearest bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 5
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : N
  Device Type                 : Not Defined
 Traffic statistics           :
  Total frames transmitted    : 4
  Total entries aged          : 0
  Total frames received       : 3
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
```

Customer Bridge

All configuration commands in the table below should be followed for each switch.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent customer-bridge`	Enter into the Customer Bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#set lldp chassis-id-tlv ip-address`	Configure the subtype for chassis-id TLV
`(if-lldp-agent)#set lldp port-id-tlv mac-address`	Configure the subtype for port-id TLV

`(if-lldp-agent)#lldp tlv basic-mgmt port-description select`	Enable the port-description TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv basic-mgmt system-name select`	Enable the system-name TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv basic-mgmt system-capabilities select`	Enable the system-capabilities TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv basic-mgmt system-description select`	Enable the system-description TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv basic-mgmt management-address select`	Enable the management-address TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-vlanid select`	Enable the VLAN-id TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vlan-name select`	Enable the VLAN-NAME TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-ptcl-vlanid select`	Enable the Port and Protocol VLAN id TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific ptcl-identity select`	Enable the Protocol Identity TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vid-digest select`	Enable the VID Usage Digest TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific mgmt-vid select`	Enable the Management VID TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific link-agg select`	Enable the Link Aggregation TLV to be transmitted on the port.
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific mac-phy select`	Enable the MAC/PHY Configuration/Status TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific max-mtu-size select`	Enable the Maximum Frame Size TLV to be transmitted on the port.
`(if-lldp-agent)#set lldp timer msg-fast-tx 5`	Defines the time interval during fast transmission periods.
`(if-lldp-agent)#set lldp tx-fast-init 6`	Defines the number of LLD PDUs that are transmitted during a fast transmission period.
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#commit`	Commit the candidate configuration to the running configuration.
`(config-if)#exit`	Exit interface mode.

Validation

1. Verify the LLDP configurations in the local switch:

```
#show #show running-config lldp
!
interface eth1
lldp-agent customer-bridge
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
  set lldp port-id-tlv mac-address
  lldp tlv basic-mgmt port-description select
  lldp tlv basic-mgmt system-name select
  lldp tlv basic-mgmt system-description select
  lldp tlv basic-mgmt system-capabilities select
```

```
  lldp tlv basic-mgmt management-address select
  lldp tlv ieee-8021-org-specific port-vlanid select
  lldp tlv ieee-8021-org-specific port-ptcl-vlanid select
  lldp tlv ieee-8021-org-specific vlan-name select
  lldp tlv ieee-8021-org-specific ptcl-identity select
  lldp tlv ieee-8021-org-specific vid-digest select
  lldp tlv ieee-8021-org-specific mgmt-vid select
  lldp tlv ieee-8021-org-specific link-agg select
  lldp tlv ieee-8023-org-specific mac-phy select
  lldp tlv ieee-8023-org-specific max-mtu-size select
  set lldp timer msg-fast-tx 5
  set lldp tx-fast-init 6
!
```

2. Verify the LLDP port statistics

```
#show lldp interface eth1 customer-bridge

Agent Mode                    : Customer-bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 5
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : N
  Device Type                 : Not Defined
 Traffic statistics           :
  Total frames transmitted    : 8
  Total entries aged          : 0
  Total frames received       : 7
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
```

Non-Tpmr-Bridge

The below configurations should be followed for each switch.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent non-tpmr-bridge`	Enter into the Non tpmr Bridge agent
`(if-lldp-agent)#set lldp enable txrx`	Enable an LLDP agent on the port.
`(if-lldp-agent)#set lldp chassis-id-tlv ip-address`	Configure the subtype for chassis-id TLV

`(if-lldp-agent)#set lldp port-id-tlv mac-address`	Configure the subtype for port-id TLV
`(if-lldp-agent)#lldp tlv basic-mgmt port-description select`	Enable the port-description TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt system-name select`	Enable the system-name TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt system-capabilities select`	Enable the system-capabilities TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt system-description select`	Enable the system-description TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv basic-mgmt management-address select`	Enable the management-address TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-vlanid select`	Enable the VLAN-id TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vlan-name select`	Enable the VLAN-NAME TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-ptcl-vlanid select`	Enable the Port and Protocol VLAN id TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific ptcl-identity select`	Enable the Protocol Identity TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific vid-digest select`	Enable the VID Usage Digest TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific mgmt-vid select`	Enable the Management VID TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8021-org-specific link-agg select`	Enable the Link Aggregation TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific mac-phy select`	Enable the MAC/PHY Configuration/Status TLV to be transmitted on the port
`(if-lldp-agent)#lldp tlv ieee-8023-org-specific max-mtu-size select`	Enable the Maximum Frame Size TLV to be transmitted on the port
`(if-lldp-agent)#set lldp timer msg-fast-tx 5`	Defines the time interval during fast transmission periods
`(if-lldp-agent)#set lldp tx-fast-init 6`	Defines the number of LLD PDUs that are transmitted during a fast transmission period
`(if-lldp-agent)#exit`	Exit the lldp agent mode
`(config-if)#commit`	Commit the candidate configuration to the running configuration.
`(config-if)#exit`	Exit interface mode.

Validation

1. Verify the LLDP configurations in the local switch:

```
#show running-config lldp
lldp-agent non-tpmr-bridge
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
  set lldp port-id-tlv mac-address
  lldp tlv basic-mgmt port-description select
  lldp tlv basic-mgmt system-name select
  lldp tlv basic-mgmt system-description select
  lldp tlv basic-mgmt system-capabilities select
```

```
  lldp tlv basic-mgmt management-address select
  lldp tlv ieee-8021-org-specific port-vlanid select
  lldp tlv ieee-8021-org-specific port-ptcl-vlanid select
  lldp tlv ieee-8021-org-specific vlan-name select
  lldp tlv ieee-8021-org-specific ptcl-identity select
  lldp tlv ieee-8021-org-specific vid-digest select
  lldp tlv ieee-8021-org-specific mgmt-vid select
  lldp tlv ieee-8021-org-specific link-agg select
  lldp tlv ieee-8023-org-specific mac-phy select
  lldp tlv ieee-8023-org-specific max-mtu-size select
  set lldp timer msg-fast-tx 5
  set lldp tx-fast-init 6

!
```

2. Verify the LLDP port statistics

```
#show lldp interface eth1 non-tmpr-bridge

Agent Mode                    : Non-TPMR-bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 5
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : Y
  Device Type                 : Not Defined
 Traffic statistics           :
  Total frames transmitted    : 17
  Total entries aged          : 0
  Total frames received       : 6
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
```

Media Endpoint Devices TLV

Switch A

`(config)#interface eth1`	Enter interface mode.
`(config-if)#lldp-agent`	Enter the default agent.
`(if-lldp-agent)#set lldp enable txrx`	Set the admin status of the LLDP agent.
`(if-lldp-agent)#exit`	Exit agent mode.
`(config-if)#lldp-agent customer-bridge`	Enter the customer-bridge agent.
`(if-lldp-agent)#set lldp enable txrx`	Set the admin status of the LLDP agent.
`(if-lldp-agent)#exit`	Exit agent mode.
`(config-if)#lldp-agent non-tpmr-bridge`	Enter the non-tpmr-bridge agent.
`(if-lldp-agent)#set lldp enable txrx`	Set the admin status of the LLDP agent.
`(if-lldp-agent)#exit`	Exit agent mode.
`(config-if)#set lldp med-devtype net-connect`	Enter the med-devtype agent and set the device type to network connectivity.

(config-if)#exit	Exit agent mode.
(config-if)#commit	Commit the candidate configuration to the running configuration.

Validation

```
#show run lldp
!
!
interface eth1
 lldp-agent
  set lldp enable txrx
 set lldp med-devtype net-connect
 lldp-agent non-tpmr-bridge
  set lldp enable txrx
 lldp-agent customer-bridge
  set lldp enable txrx
!
#

#show lldp interface eth1
Agent Mode                   : Customer-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : Y
  Device Type                : Network Connectivity
 Traffic statistics          :
  Total frames transmitted   : 97
  Total entries aged         : 1
  Total frames received      : 92
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
Agent Mode                   : Non-TPMR-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : N
  Device Type                : Network Connectivity
 Traffic statistics          :
  Total frames transmitted   : 89
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
```

```
Agent Mode                    : Nearest bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 1
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : N
  Device Type                 : Network Connectivity
 Traffic statistics           :
  Total frames transmitted    : 90
  Total entries aged          : 0
  Total frames received       : 0
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
#
```

Switch B

`(config)#interface eth1`	Enter interface mode.
`(config-if)#lldp-agent`	Enter the default agent.
`(if-lldp-agent)#set lldp enable txrx`	Set the admin status of the LLDP agent.
`(if-lldp-agent)#exit`	Exit agent mode.
`(config-if)#lldp-agent customer-bridge`	Enter the customer-bridge agent.
`(if-lldp-agent)#set lldp enable txrx`	Set the admin status of the LLDP agent.
`(if-lldp-agent)#exit`	Exit agent mode.
`(config-if)#lldp-agent non-tpmr-bridge`	Enter the non-tpmr-bridge agent.
`(if-lldp-agent)#set lldp enable txrx`	Set the admin status of the LLDP agent.
`(if-lldp-agent)#exit`	Exit agent mode.
`(config-if)#set lldp med-devtype ep-class3`	Enter the med-devtype agent and set the device type to endpoint class 3.
`(config-if)#exit`	Exit agent mode.
`(config-if)#commit`	Commit the candidate configuration to the running configuration.

Validation

```
#show running-config lldp
!
!
interface eth1
 lldp-agent
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
 set lldp med-devtype ep-class3
 lldp-agent non-tpmr-bridge
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
 lldp-agent customer-bridge
```

```
  set lldp enable txrx
  set lldp chassis-id-tlv ip-address
!
#

#show lldp interface eth1
Agent Mode                    : Customer-bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 1
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : Y
  Device Type                 : End Point Class-3
 Traffic statistics           :
  Total frames transmitted    : 11
  Total entries aged          : 0
  Total frames received       : 12
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
Agent Mode                    : Non-TPMR-bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 1
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : Y
  Device Type                 : End Point Class-3
 Traffic statistics           :
  Total frames transmitted    : 7
  Total entries aged          : 0
  Total frames received       : 0
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
Agent Mode                    : Nearest bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 1
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : Y
  Device Type                 : End Point Class-3
 Traffic statistics           :
  Total frames transmitted    : 8
  Total entries aged          : 0
  Total frames received       : 0
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
```

```
  Total unrecognised TLVs     : 0
#
```

Global Mode TLV

LLDPv2 TLVs can be configured globally, making it applicable for all interfaces where LLDP is enabled.

Topology

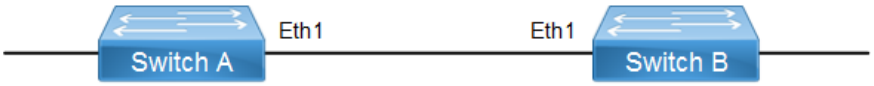


Figure 1-2: LLDP topology

SW1

`SW1#configure terminal`	Enter Configure mode
`SW1(config)#lldp tlv-select basic-mgmt port-description`	Enable LLDP port description TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt system-name`	Enable LLDP system name TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt system-capabilities`	Enable LLDP system capabilities TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt system-description`	Enable LLDP system description TLV in global mode
`SW1(config)#lldp tlv-select basic-mgmt management-address`	Enable LLDP management address TLV in global mode
`SW1(config)#interface eth1`	Enter interface mode
`SW1(config-if)#lldp-agent`	Enter LLDP interface mode
`SW1(if-lldp-agent)#set lldp enable txrx`	Enable LLDP TLV transmit and receive for the nearest bridge
`SW1(if-lldp-agent)#exit`	Exit LLDP mode
`SW1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#end`	Exit the configure mode

SW2

`SW2#configure terminal`	Enter Configure mode
`SW2(config)#lldp tlv-select basic-mgmt port-description`	Enable LLDP port description TLV in global mode
`SW2(config)#lldp tlv-select basic-mgmt system-name`	Enable LLDP system name TLV in global mode
`SW2(config)#lldp tlv-select basic-mgmt system-capabilities`	Enable LLDP system capabilities TLV in global mode
`SW2(config)#lldp tlv-select basic-mgmt system-description`	Enable LLDP system description TLV in global mode

`SW2(config)#lldp tlv-select basic-mgmt management-address`	Enable LLDP management address TLV in global mode
`SW2(config)#interface eth1`	Enter interface mode
`SW2(config-if)#lldp-agent`	Enter LLDP interface mode
`SW2(if-lldp-agent)#set lldp enable txrx`	Enable LLDP TLV transmit and receive for the nearest bridge
`SW2(if-lldp-agent)#exit`	Exit LLDP mode
`SW2(config-if)#commit`	Commit the candidate configuration to the running configuration.
`SW2(config-if)#exit`	Exit interface mode
`SW2(config)#end`	Exit the configure mode

Validation

```
SW1#show running-config lldp
!
lldp tlv-select basic-mgmt port-description
lldp tlv-select basic-mgmt system-name
lldp tlv-select basic-mgmt system-capabilities
lldp tlv-select basic-mgmt system-description
lldp tlv-select basic-mgmt management-address
!
interface eth1
 lldp-agent
  set lldp enable txrx


SW1#show lldp neighbors

Loc PortID      Rem Host Name      Rem Chassis Id     Rem Port Id       Agent Mode

--------------------------------------------------------------------------------
Eth1           OcNOS              cc37.ab56.6d80     cc37.abbb.ed81    Nearest bridge


SW1#show lldp neighbors detail

--------------------------------------------------------------------------------

Nearest bridge Neighbors
Interface Name              : eth1
 Mandatory TLVs
 Chassis id type          : MAC address [cc37.ab56.6d80]
 Port id type             : MAC address [cc37.abbb.ed81]
 Time to live             : 121
 Basic Management TLVs
 System Name              : SW2
 System Description       : Hardware Model:EC_AS4610-54, Software version: Oc
NOS,1.3.6.241a
 Port Description          : eth1
```

```
 Remote System Capabilities : Bridge
                              Router
 Capabilities Enabled     : Router
 Management Address        : MAC Address [cc37.abbb.ed81]
 Interface Number subtype  : ifindex
 Interface Number          10046
 OID Number              : 0
 802.1 Org specific TLVs
 Port vlan id              : 0
 Port & Protocol vlan id   : 0
 Remote Configured VLANs   : None
 Remote Protocols Advertised: None
 Remote VID Usage Digest   : 0
 Remote Management Vlan    : 0
 Link Aggregation Capability: not capable of being aggregated
 Link Aggregation Status   : not currently in aggregation
 Link Aggregation Port ID  :
 802.3 Org specific TLVs
 AutoNego Support          : Not-Supported
 AutoNego Status           : Disabled
 AutoNego Capability       : 0
 Operational MAU Type      : 0 [unknown]
  Max Frame Size            :
SW1#
```

LLDP-MED

LLDP extensions and behavior requirements are described specifically in the areas of network Configuration and policy, device location (including for Emergency Call Service / E911), Power over Ethernet management, and inventory management.

Based on the device type, different TLVs are advertised by the Station.

LLDP-MED Network Connectivity Device

LLDP-MED Network Connectivity Devices, as defined in this Standard, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

- LAN Switch/Router
- IEEE 802.1 Bridge
- IEEE 802.3 Repeater (included for historical reasons)
- IEEE 802.11 Wireless Access Point
- Any device that supports the IEEE 802.1AB and MED extensions defined by this Standard and can relay IEEE 802 frames via any method.

Configuration Command

```
set lldp med-devtype net-connect
```

LLDP-MED Generic Endpoint (Class I)

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services.

Configuration command:

```
set lldp med-devtype ep-class1
```

LLDP-MED Generic Endpoint (Class 2)

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar

Configuration command:

```
set lldp med-devtype ep-class2
```

LLDP-MED Generic Endpoint (Class 3)

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Configuration command:

```
set lldp med-devtype ep-class3
```

Switch A

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure an IEEE VLAN-aware bridge.
`(config)#vlan database`	Enter VLAN configure mode.
`(config-vlan)#vlan 2 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`(config-vlan)#exit`	Exit the VLAN configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Set switching characteristics on the port.
`(config-if)#bridge-group 1`	Associate the interface to the bridge.
`(config-if)#lldp-agent`	Enter into the default agent

(if-lldp-agent)#set lldp enable txrx	Enable an LLDP agent on the port.
(if-lldp-agent)#exit	Exit the lldp agent mode
(if-config-if)#lldp-agent customer-bridge	Enter into the customer-bridge agent.
(if-lldp-agent)#set lldp enable txrx	Enable an LLDP agent on the port.
(if-lldp-agent)#exit	Exit the lldp agent mode
(config-if)#lldp-agent non-tpmr-bridge	Enter into the non-tpmr-bridge agent
(if-lldp-agent)#set lldp enable txrx	Enable an LLDP agent on the port.
(if-lldp-agent)#exit	Exit the lldp agent mode
(config-if)#set lldp med-devtype net-connect	Configure the med device type
(config-if)#exit	Exit interface mode.
(config-if)#commit	Commit the candidate configuration to the running configuration.

Switch B

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol ieee vlan-bridge	Configure an IEEE VLAN-aware bridge.
(config)#vlan database	Enter VLAN configure mode.
(config-vlan)#vlan 2 bridge 1 state enable	Configure a VLAN and add it to the bridge.
(config-vlan)#exit	Exit the VLAN configuration mode.
(config)#interface eth1	Enter interface mode.
(config-if)#switchport	Set switching characteristics on the port.
(config-if)#bridge-group 1	Associate the interface to the bridge.
(config-if)#lldp-agent	Enter into the default agent
(if-lldp-agent)#set lldp enable txrx	Enable an LLDP agent on the port.
(if-lldp-agent)#exit	Exit the lldp agent mode
(config-if)#lldp-agent customer-bridge	Enter into the customer-bridge agent
(if-lldp-agent)#set lldp enable txrx	Enable an LLDP agent on the port.
(if-lldp-agent)#exit	Exit the lldp agent mode
(config-if)#lldp-agent non-tpmr-bridge	Enter into the non-tpmr-bridge agent
(if-lldp-agent)#set lldp enable txrx	Enable an LLDP agent on the port.
(if-lldp-agent)#exit	Exit the lldp agent mode
(config-if)#set lldp med-devtype ep-class3	Configure the med device type
(config-if)#exit	Exit interface mode.
(config-if)#commit	Commit the candidate configuration to the running configuration.

Validation

1. Verify the LLDP configurations on Switch A:

```
#show running-config lldp
!
!
interface eth1
 lldp-agent
  set lldp enable txrx
 set lldp med-devtype net-connect
 lldp-agent non-tpmr-bridge
  set lldp enable txrx
 lldp-agent customer-bridge
  set lldp enable txrx
!
```

2. Verify the LLDP port statistics on Switch A:

```
#show lldp interface eth1
Agent Mode                    : Customer-bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 1
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : Y
  Device Type                 : Network Connectivity
 Traffic statistics           :
  Total frames transmitted    : 11
  Total entries aged          : 0
  Total frames received       : 10
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
Agent Mode                    : Non-TPMR-bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 1
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : N
  Device Type                 : Network Connectivity
 Traffic statistics           :
  Total frames transmitted    : 7
  Total entries aged          : 0
  Total frames received       : 0
  Total error frames received: 0
  Total frames discarded      : 0
  Total discarded TLVs        : 0
  Total unrecognised TLVs     : 0
Agent Mode                    : Nearest bridge
 Enable (tx/rx)               : Y/Y
 Message fast transmit time   : 1
 Message transmit interval    : 30
 Reinitialisation delay       : 2
 MED Enabled                  : N
  Device Type                 : Network Connectivity
 Traffic statistics           :
```

```
  Total frames transmitted   : 7
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0

#show lldp interface eth1 non-tpmr-bridge
Agent Mode                   : Non-TPMR-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 5
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : N
  Device Type                : Not Defined
 Traffic statistics          :
  Total frames transmitted   : 4
  Total entries aged         : 0
  Total frames received      : 0
  Total error frames received: 0
  Total frames discarded     : 0
  Total discarded TLVs       : 0
  Total unrecognised TLVs    : 0
```

3. Verify the LLDP configurations for end device ep-class3 on Switch B:

```
#show running-config lldp
!
interface eth1
 set lldp med-devtype ep-class3
 lldp-agent
  set lldp enable txrx
  lldp tlv med network-policy select
lldp-agent non-TPMR-bridge
  set lldp enable txrx
  lldp tlv med network-policy select
lldp-agent customer-bridge
  set lldp enable txrx
  lldp tlv med network-policy select
!
```

4. Verify the LLDP port statistics on Switch B:

```
#show lldp interface eth1
Agent Mode                   : Customer-bridge
 Enable (tx/rx)              : Y/Y
 Message fast transmit time  : 1
 Message transmit interval   : 30
 Reinitialisation delay      : 2
 MED Enabled                 : Y
  Device Type                : End Point Class-3
 Traffic statistics          :
  Total frames transmitted   : 124
  Total entries aged         : 0
  Total frames received      : 125
  Total error frames received: 0
  Total frames discarded     : 0
```

```
    Total discarded TLVs       : 0
    Total unrecognised TLVs    : 0
  Agent Mode                   : Non-TPMR-bridge
   Enable (tx/rx)              : Y/Y
   Message fast transmit time  : 1
   Message transmit interval   : 30
   Reinitialisation delay      : 2
   MED Enabled                 : Y
    Device Type                : End Point Class-3
   Traffic statistics          :
    Total frames transmitted   : 120
    Total entries aged         : 0
    Total frames received      : 0
    Total error frames received: 0
    Total frames discarded     : 0
    Total discarded TLVs       : 0
    Total unrecognised TLVs    : 0
  Agent Mode                   : Nearest bridge
   Enable (tx/rx)              : Y/Y
   Message fast transmit time  : 1
   Message transmit interval   : 30
   Reinitialisation delay      : 2
   MED Enabled                 : Y
    Device Type                : End Point Class-3
   Traffic statistics          :
    Total frames transmitted   : 120
    Total entries aged         : 0
    Total frames received      : 0
    Total error frames received: 0
    Total frames discarded     : 0
    Total discarded TLVs       : 0
    Total unrecognised TLVs    : 0
  #
```

LLDP Over SVI, LAG, and Sub-Interface

Overview

Link Layer Discovery Protocol (LLDP) is an open-source Layer 2 protocol that runs on the data link layer. It is a neighbor discovery protocol that defines a method for network access devices using Ethernet connectivity to advertise themselves to other devices on the same physical LAN and then store information about the network. It allows a device to learn higher-layer management reachability and connection endpoint information from adjacent devices. Using LLDP, a network device can advertise its identity, capabilities, and media-specific configuration and learn the same information.

LLDP supports a set of defined attributes used to find neighboring devices includeing:

- T- type
- L- length
- V- value descriptions

The information is transmitted and/or received by neighbor devices through each of their LLDP-enabled interfaces, which send Ethernet frames at regular intervals. The Management Address TLV in LLDP identifies an address (MAC or Layer3 IP) associated with the local LLDP agent used to reach higher-layer entities to assist discovery by network

management. This TLV also provides room for the inclusion of the system interface number and an object identifier (OID) associated with this management address.

Feature Characteristics

LLDP enabled devices are capable of:

- Discovering neighboring devices.
- Using as an open standard protocol.
- Sharing details about their layer-2 configurations with neighboring devices.

Benefits

- LLDP neighbor are used for SVI,LAG, and Sub Interface.
- LLDP is easy for devices to broadcast and identify information across networks.

Prerequisites

- Upon logging into the OcNOS environment enable LLDP run command on global mode.
- The enabled device should support the LLDP sub-interface configuration.

Note: Before configuring the SVI interface, ensure the physical connection between the switches is active, and ports are in the trunk mode.

Topology

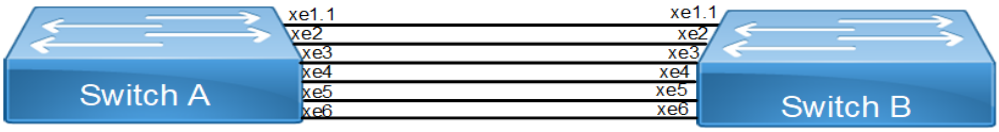


Figure 1-3: LLDP topology

Configuration

Provide the following:

1. Enter the configuration mode and configure VLAN interface.

```
SW1(#config)terminal
SW1(config)#bridge 1 protocol ieee vlan-bridge
SW1(config)#vlan database
SW1(config-vlan)#vlan 2-200 bridge 1 state enable
SW1(config-vlan)#commit
SW1(config-if)#int xe7
SW1(config-if)#switchport
SW1(config-if)#bridge-group 1
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan all
SW1(config-if)#commit

SW2(config)#bridge 1 protocol ieee vlan-bridge
SW2(config)#vlan database
```

```
SW2(config-vlan)#vlan 2-200 bridge 1 state enable
SW2(config-vlan)#commit
SW2(config)#int xe7
SW2(config-if)#switchport
SW2(config-if)#bridge-group 1
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport trunk allowed vlan all
SW2(config-if)#commit
```

2. Configure the SVLAN interface and assign the IP address to the interface.

```
SW1(config)#interface vlan1.20
SW1(config-if)#ip vrf forwarding management
SW1(config-if)#ip address 3.3.3.3/24
SW1(config-if)#commit
SW2(config)#interface vlan1.20
SW2(config-if)#ipvrf forwarding management
SW2(config-if)#ip address 3.3.3.2/24
SW2(config-if)#commit
```

3. Configure the port channel interface and assign the IP address. Connect the interfaces to the port channel.

```
SW1(config)#interface po10
SW1(config-if)#ip address 1.1.1.1/24
SW1(config-if)# ip vrf forwarding management
SW1(config-if)#commit Feature Name
SW1(config-if)#exit

SW1(config)#int xe2
SW1(config-if)#switchport
SW1(config-if)#no switchport
SW1(config-if)#channel-group 10 mode active
SW1(config-if)#commit

SW1(config)#int xe3
SW1(config-if)#switchport
SW1(config-if)#no switchport
SW1(config-if)#channel-group 10 mode active
SW1(config-if)#commit

SW1(config)#int xe4
SW1(config-if)#switchport
SW1(config-if)#no switchport
SW1(config-if)#channel-group 10 mode active
SW1(config-if)#commit

SW2(config)#interface po10
SW2(config-if)#ip address 1.1.1.2/24
SW2(config-if)# ip vrf forwarding management
SW2(config-if)#commit
SW2(config-if)#exit

SW2(config)#int xe2
SW2(config-if)#switchport
SW2(config-if)#no switchport
SW2(config-if)#channel-group 10 mode active
SW2(config-if)#commit
```

```
SW2(config)#int xe3
SW2(config-if)#switchport
SW2(config-if)#no switchport
SW2(config-if)#channel-group 10 mode active
SW2(config-if)#commit

SW2(config)#int xe4
SW2(config-if)#switchport
SW2(config-if)#no switchport
SW2(config-if)#channel-group 10 mode active
```

4. Configure sub interfaces on both SW1 and SW2, and assign the IP address to the interfaces.

```
SW1(config)#int xe6.10
SW1(config-if)#encapsulation dot1q 10
SW1(config-if)#ip address 2.2.2.3/24
SW1(config-if)#ip vrf forwarding management
SW1(config-if)#commit

SW2(config)#int xe6.10
SW2(config-if)#encapsulation dot1q 10
SW2(config-if)#ip address 2.2.2.2/24
SW2(config-if)#ip vrf forwarding management
SW2(config-if)#commit
```

5. Enable the LLDP agent mode and capabilities on both switch interfaces.

```
SW1(config)#int xe6
SW1(config-if)#lldp-agent customer-bridge
SW1(if-lldp-agent)#set lldp enable txrx
SW1(if-lldp-agent)#set lldp chassis-id-tlv ip-address
SW1(if-lldp-agent)#lldp tlv basic-mgmt management-address select
SW1(if-lldp-agent)#commit

SW2(config-if)#int xe6
SW2(config-if)# lldp-agent
SW2(if-lldp-agent)#set lldp enable txrx
SW2(if-lldp-agent)#set lldp management-address-tlv ip-address
SW2(if-lldp-agent)#lldp tlv basic-mgmt management-address select
SW2(if-lldp-agent)#commit
```

6. Verify the LLDP neighbors on the device.

```
SW1 show lldp int xe6 neighbor

Nearest bridge Neighbors
Interface Name : xe6
Mandatory TLVs
Chassis id type : MAC address [b86a.9782.1fba]
Port id type : MAC address [b86a.9782.1fc1]
Time to live : 121
Basic Management TLVs
System Name :
System Description :
Port Description :
Remote System Capabilities : None
Capabilities Enabled : None
Management Address : IP Address [10.12.181.117]
```

```
Interface Number subtype : ifindex
Interface Number : 3
OID Number : 0
Management Address : IP Address [2.2.2.2]
Interface Number subtype : ifindex
Interface Number : 327876618
OID Number : 0
Management Address : IP Address [3.3.3.2]
Interface Number subtype : ifindex
Interface Number : 25020
OID Number : 0
802.1 Org specific TLVs
Port vlan id : 0
Port & Protocol vlan id : 0
Remote Configured VLANs : None
Remote Protocols Advertised: None
Remote VID Usage Digest : 0
Remote Management Vlan : 0
Link Aggregation Capability: not capable of being aggregated
Link Aggregation Status : not currently in aggregation
Link Aggregation Port ID : 802.3 Org specific TLVs
AutoNego Support : Not-Supported
AutoNego Status : Disabled
AutoNego Capability : 0
Operational MAU Type : 0 [unknown]
SW2#sh lldp int xe7 neighbor
Nearest bridge Neighbors
Interface Name : xe7

Mandatory TLVs
Chassis id type : MAC address [5c07.5828.a775]
Port id type : MAC address [5c07.5828.a77d]
Time to live : 121

Basic Management TLVs
System Name : SW1
System Description : Hardware Model:UFI_S9510-30XC,
Software version: OcNOS,6.5.1.48
Port Description : xe7
Remote System Capabilities : Bridge Router
Capabilities Enabled : Bridge Router

Management Address : MAC Address [5c07.5828.a77d]
Interface Number subtype : ifindex
Interface Number : 5008
OID Number : 0
802.1 Org specific TLVs
Port vlan id : 1
Port & Protocol vlan id : 0
```

```
Remote Configured VLANs :
vlan-id: 1 vlan-name: default
vlan-id: 2 vlan-name: VLAN0002
vlan-id: 3 vlan-name: VLAN0003
vlan-id: 4 vlan-name: VLAN0004
vlan-id: 5 vlan-name: VLAN0005
vlan-id: 6 vlan-name: VLAN0006
vlan-id: 7 vlan-name: VLAN0007
vlan-id: 8 vlan-name: VLAN0008
vlan-id: 9 vlan-name: VLAN0009
vlan-id: 10 vlan-name: VLAN0010
vlan-id: 11 vlan-name: VLAN0011
vlan-id: 12 vlan-name: VLAN0012
vlan-id: 13 vlan-name: VLAN0013
vlan-id: 14 vlan-name: VLAN0014
vlan-id: 15 vlan-name: VLAN0015
vlan-id: 16 vlan-name: VLAN0016
vlan-id: 17 vlan-name: VLAN0017
vlan-id: 18 vlan-name: VLAN0018
vlan-id: 19 vlan-name: VLAN0019
vlan-id: 20 vlan-name: VLAN0020
vlan-id: 21 vlan-name: VLAN0021
vlan-id: 22 vlan-name: VLAN0022
vlan-id: 23 vlan-name: VLAN0023
vlan-id: 24 vlan-name: VLAN0024
vlan-id: 25 vlan-name: VLAN0025
vlan-id: 26 vlan-name: VLAN0026
vlan-id: 27 vlan-name: VLAN0027
vlan-id: 28 vlan-name: VLAN0028
vlan-id: 29 vlan-name: VLAN0029
vlan-id: 30 vlan-name: VLAN0030
vlan-id: 31 vlan-name: VLAN0031
vlan-id: 32 vlan-name: VLAN0032
vlan-id: 33 vlan-name: VLAN0033
vlan-id: 34 vlan-name: VLAN0034
vlan-id: 35 vlan-name: VLAN0035
vlan-id: 36 vlan-name: VLAN0036
vlan-id: 37 vlan-name: VLAN0037
vlan-id: 38 vlan-name: VLAN0038
vlan-id: 39 vlan-name: VLAN0039
vlan-id: 40 vlan-name: VLAN0040
vlan-id: 41 vlan-name: VLAN0041
vlan-id: 42 vlan-name: VLAN0042
vlan-id: 43 vlan-name: VLAN0043
vlan-id: 44 vlan-name: VLAN0044
vlan-id: 45 vlan-name: VLAN0045
vlan-id: 46 vlan-name: VLAN0046
vlan-id: 47 vlan-name: VLAN0047
vlan-id: 48 vlan-name: VLAN0048
vlan-id: 49 vlan-name: VLAN0049
```

```
vlan-id: 50 vlan-name: VLAN0050
vlan-id: 51 vlan-name: VLAN0051
vlan-id: 52 vlan-name: VLAN0052
vlan-id: 53 vlan-name: VLAN0053
vlan-id: 54 vlan-name: VLAN0054
vlan-id: 55 vlan-name: VLAN0055
vlan-id: 56 vlan-name: VLAN0056
vlan-id: 57 vlan-name: VLAN0057
vlan-id: 58 vlan-name: VLAN0058
vlan-id: 59 vlan-name: VLAN0059
vlan-id: 60 vlan-name: VLAN0060
vlan-id: 61 vlan-name: VLAN0061
vlan-id: 62 vlan-name: VLAN0062
vlan-id: 63 vlan-name: VLAN0063
vlan-id: 64 vlan-name: VLAN0064
vlan-id: 65 vlan-name: VLAN0065
vlan-id: 66 vlan-name: VLAN0066
vlan-id: 67 vlan-name: VLAN0067
vlan-id: 68 vlan-name: VLAN0068
vlan-id: 69 vlan-name: VLAN0069
vlan-id: 70 vlan-name: VLAN0070
vlan-id: 71 vlan-name: VLAN0071
vlan-id: 72 vlan-name: VLAN0072
vlan-id: 73 vlan-name: VLAN0073
vlan-id: 74 vlan-name: VLAN0074
vlan-id: 75 vlan-name: VLAN0075
Remote Protocols Advertised: Spanning Tree Protocol
Remote VID Usage Digest : 0
Remote Management Vlan : 0
Link Aggregation Capability: capable of being aggregated
Link Aggregation Status : not currently in aggregation
Link Aggregation Port ID : 802.3 Org specific TLVs
AutoNego Support : Supported
AutoNego Status : Disabled
AutoNego Capability : 16
Operational MAU Type : 54 [Four-pair Category 6A or better, full duplex mode only]
Max Frame Size : 1522
```

Implementation Examples

Enter configuration commands.

```
SW1(config)#lldp tlv-select basic-mgmt port-description
SW1(config)# lldp tlv-select basic-mgmt system-name
SW1(config)# lldp tlv-select basic-mgmt system-description
SW1(config)# lldp tlv-select basic-mgmt system-capabilities
SW1(config)# lldp tlv-select basic-mgmt management-address
SW1(config)#
SW1(config)#
SW1(config)# lldp tlv-select ieee-8021-org-specific port-vlanid
SW1(config)# lldp tlv-select ieee-8021-org-specific port-ptcl-vlanid
SW1(config)# lldp tlv-select ieee-8021-org-specific vlan-name
```

```
SW1(config)# lldp tlv-select ieee-8021-org-specific ptcl-identity
SW1(config)# lldp tlv-select ieee-8021-org-specific vid-digest
SW1(config)# lldp tlv-select ieee-8021-org-specific mgmt-vid
SW1(config)# lldp tlv-select ieee-8021-org-specific link-agg
SW1(config)#
SW1(config)# lldp tlv-select ieee-8023-org-specific mac-phy
SW1(config)# lldp tlv-select ieee-8023-org-specific max-mtu-size
SW1(config)#commit
SW1(config)#do sh lldp int xe6 neighbor

Nearest bridge Neighbors
Interface Name : xe6
Mandatory TLVs
Chassis id type : MAC address [b86a.9782.1fba]
Port id type : MAC address [b86a.9782.1fc1]
Time to live : 121
Basic Management TLVs
System Name : SW2
System Description : Hardware Model:EC_AS5912-54X, Software version:
OcNOS,6.5.1.49
Port Description : xe6
Remote System Capabilities : Bridge
Router
Capabilities Enabled : Bridge
Router
Management Address : IP Address [10.12.181.117]
Interface Number subtype : ifindex
Interface Number : 3
OID Number : 0
Management Address : IP Address [2.2.2.2]
Interface Number subtype : ifindex
Interface Number : 327876618
OID Number : 0
Management Address : IP Address [3.3.3.2]
Interface Number subtype : ifindex
Interface Number : 25020
OID Number : 0
802.1 Org specific TLVs
Port vlan id : 0
Port & Protocol vlan id : 0
Remote Configured VLANs : None
Remote Protocols Advertised: None
Remote VID Usage Digest : 0
Remote Management Vlan : 0 Feature Name
Link Aggregation Capability: capable of being aggregated
Link Aggregation Status : not currently in aggregation
Link Aggregation Port ID :
802.3 Org specific TLVs
AutoNego Support : Supported
AutoNego Status : Disabled
AutoNego Capability : 16
Operational MAU Type : 54 [Four-pair Category 6A or better, full duplex mode
only]
Max Frame Size : 1518
SW1(config)# end
```

CHAPTER 2 Provider Bridging Configuration

This chapter contains sample provider bridging configurations.

A provider bridged network is a virtual bridged Local Area Network that comprises provider bridges (SVLAN bridges and provider edge bridges) and attached LANs, under the administrative control of a single service provider. Provider bridges interconnect the separate MACs of the IEEE 802 LANs that compose a provider bridged network, relaying frames to provide connectivity between all the LANs that provide customer interfaces for each service instance.

Single Provider Bridge Configuration

Topology

Figure 2-4: Single provider bridge configuration

Configuration

SW1 (PEB)

`SW1#configure terminal`	Enter configuration mode
`SW1(config)#bridge 1 protocol provider-rstp edge`	Create bridge
`SW1(config)#vlan database`	Enter VLAN configuration mode
`SW1(config-vlan)#vlan 2 type customer bridge 1 state enable`	Create customer vlan VLAN 2
`SW1(config-vlan)#vlan 200 type service point-point bridge 1 state enable`	Create service vlan VLAN200
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#cvlan registration table map1 bridge 1`	Create cvlan registration table map1
`SW1(config-cvlan-registration)#cvlan 2 svlan 200`	Map cvlan2 with svlan 200
`SW1(config-cvlan-registration)#exit`	Exit registration table
`SW1(config)#interface eth1`	Enter interface configuration mode for eth1
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode customer-edge hybrid`	Configure switchport mode customer edge
`SW1(config-if)#switchport customer-edge access vlan 2`	Associate customer vlan2 with interface

`SW1(config-if)#switchport customer-edge vlan registration map1`	Attach registration table map1 with interface
`SW1(config-if)#exit`	Exit interface mode
`SW1(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW1(config-if)#switchport`	Make interface as switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW1(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW1(config-if)#commit`	Commit the configuration.
`SW1(config-if)#exit`	Exit interface configuration mode

SW2 (PB)

`SW2#configure terminal`	Enter configuration mode
`SW2(config)#bridge 1 protocol provider-rstp`	Create provider bridge
`SW2(config)#vlan database`	Enter VLAN configuration mode
`SW2(config-vlan)#vlan 200 type service point-point bridge 1 state enable`	Create service vlan VLAN200
`SW2(config-vlan)#exit`	Exit VLAN configuration mode
`SW2(config)#interface eth1`	Enter interface configuration mode for eth1
`SW2(config-if)#switchport`	Make interface as switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW2(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW2(config-if)#exit`	Exit interface configuration mode
`SW2(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW2(config-if)#switchport`	Make interface as switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW2(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW2(config-if)#commit`	Commit the configuration.
`SW2(config-if)#exit`	Exit interface configuration mode

SW3 (PEB)

`SW3#configure terminal`	Enter configuration mode
`SW3(config)#bridge 1 protocol provider-rstp edge`	Create bridge
`SW3(config)#vlan database`	Enter VLAN configuration mode

`SW3(config-vlan)#vlan 2 type customer bridge 1 state enable`	Create customer vlan VLAN 2
`SW3(config-vlan)#vlan 200 type service point-point bridge 1 state enable`	Create service vlan VLAN200
`SW3(config-vlan)#exit`	Exit VLAN configuration mode
`SW3(config)#cvlan registration table map1 bridge 1`	Create cvlan registration table map1
`SW3(config-cvlan-registration)#cvlan 2 svlan 200`	Map cvlan2 with svlan 200
`SW3(config-cvlan-registration)#exit`	Exit registration table
`SW3(config)#interface eth1`	Enter interface configuration mode for eth1
`SW3(config-if)#switchport`	Configure switchport
`SW3(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW3(config-if)#witchport mode customer-edge hybrid`	Configure switchport mode customer edge
`SW3(config-if)#switchport customer-edge access vlan 2`	Associate customer vlan2 with interface
`SW3(config-if)#switchport customer-edge vlan registration map1`	Attach registration table map1 with interface
`SW3(config-if)#exit`	Exit interface mode
`SW3(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW3(config-if)#switchport`	Make interface as switchport
`SW3(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW3(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW3(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW3(config-if)#commit`	Commit the configuration.
`SW3(config-if)#exit`	Exit interface configuration mode

Validation

```
SW3#sh br
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+------------------+-----+---------+
 1          2      200           eth1         0000.0000.0f00    1     300
 1          2      200           eth2         0001.0000.0800    1     300

SW1#sh br
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+------------------+-----+---------+
 1          2      200           eth2         0000.0000.0f00    1     300
```

```
 1          2      200           eth1       0001.0000.0800    1     300

SW1#sh cvlan registration table
Bridge          Table Name       Port List

======          ==========       =========

1               map1             eth1

CVLAN ID        SVLAN ID
========        ========
2               200
```

Two Provider Bridge Configuration

Topology

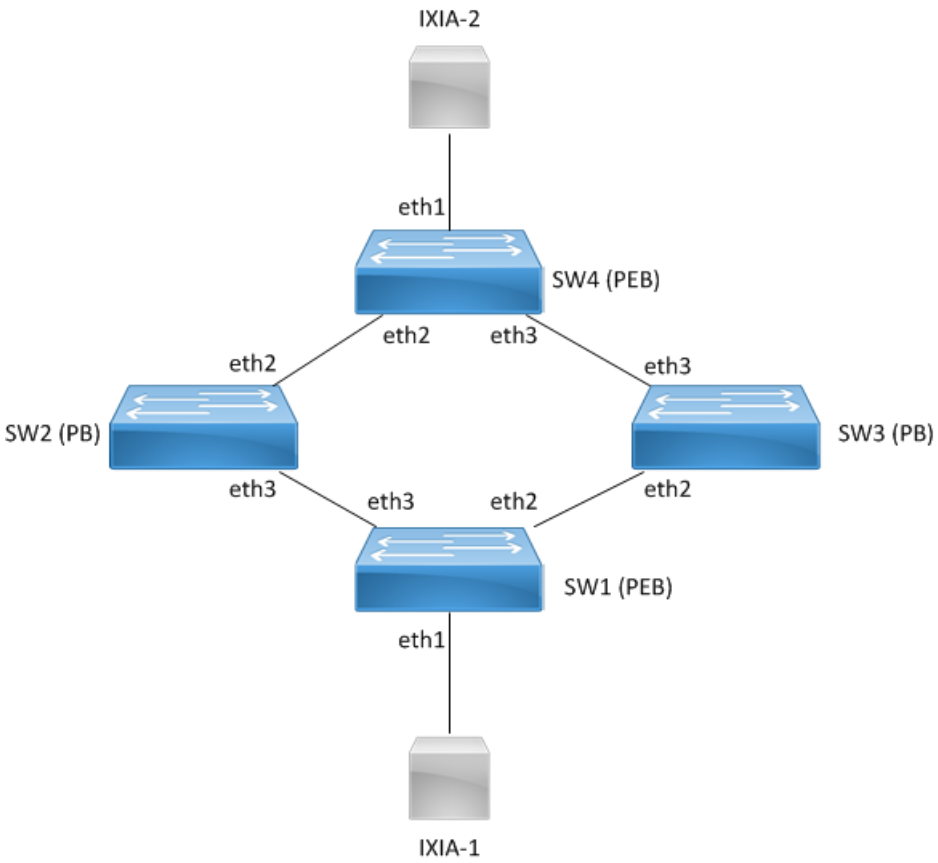


Figure 2-5: Two provider bridge configuration

Configuration

SW1 (PEB)

`SW1#configure terminal`	Enter configuration mode
`SW1(config)#bridge 1 protocol provider-rstp edge`	Create bridge
`SW1(config)#vlan database`	Enter VLAN configuration mode
`SW1(config-vlan)#vlan 2 type customer bridge 1 state enable`	Create customer vlan VLAN 2
`SW1(config-vlan)#vlan 200 type service point-point bridge 1 state enable`	Create service vlan VLAN200
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#cvlan registration table map1 bridge 1`	Create cvlan registration table map1
`SW1(config-cvlan-registration)#cvlan 2 svlan 200`	Map cvlan2 with svlan 200
`SW1(config-cvlan-registration)#exit`	Exit registration table
`SW1(config)#interface eth1`	Enter interface configuration mode for eth1
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#witchport mode customer-edge hybrid`	Configure switchport mode customer edge
`SW1(config-if)#switchport customer-edge access vlan 2`	Associate customer vlan2 with interface
`SW1(config-if)#switchport customer-edge vlan registration map1`	Attach registration table map1 with interface
`SW1(config-if)#exit`	Exit interface mode
`SW1(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW1(config-if)#switchport`	Make interface as switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW1(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW1(config-if)#interface eth3`	Enter interface configuration mode for eth2
`SW1(config-if)#switchport`	Make interface as switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW1(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW1(config-if)#commit`	Commit the configuration.
`SW1(config-if)#exit`	Exit interface configuration mode

SW2 (PB)

`SW2#configure terminal`	Enter configuration mode
`SW2(config)#bridge 1 protocol provider-rstp`	Create provider bridge
`SW2(config)#vlan database`	Enter VLAN configuration mode
`SW2(config-vlan)#vlan 200 type service point-point bridge 1 state enable`	Create service vlan VLAN200
`SW2(config-vlan)#exit`	Exit VLAN configuration mode
`SW2(config)#interface eth3`	Enter interface configuration mode for eth1
`SW2(config-if)#switchport`	Make interface as switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW2(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW2(config-if)#exit`	Exit interface configuration mode
`SW2(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW2(config-if)#switchport`	Make interface as switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW2(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW2(config-if)#commit`	Commit the configuration.
`SW2(config-if)#exit`	Exit interface configuration mode

SW3 (PB)

`SW3#configure terminal`	Enter configuration mode
`SW3(config)#bridge 1 protocol provider-rstp`	Create provider bridge
`SW3(config)#vlan database`	Enter VLAN configuration mode
`SW3(config-vlan)#vlan 200 type service point-point bridge 1 state enable`	Create service vlan VLAN200
`SW3(config-vlan)#exit`	Exit VLAN configuration mode
`SW3(config)#interface eth3`	Enter interface configuration mode for eth1
`SW3(config-if)#switchport`	Make interface as switchport
`SW3(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW3(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW3(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW3(config-if)#exit`	Exit interface configuration mode
`SW3(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW3(config-if)#switchport`	Make interface as switchport

SW3(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW3(config-if)#switchport mode provider-network	Configure switchport pnp port
SW3(config-if)#switchport provider-network allowed vlan all	Associate all svlan to the port
SW3(config-if)#commit	Commit the configuration.
SW3(config-if)#exit	Exit interface configuration mode

SW4 (PEB)

SW4#configure terminal	Enter configuration mode
SW4(config)#bridge 1 protocol provider-rstp edge	Create bridge
SW4(config)#vlan database	Enter VLAN configuration mode
SW4(config-vlan)#vlan 2 type customer bridge 1 state enable	Create customer vlan VLAN 2
SW4(config-vlan)#vlan 200 type service point-point bridge 1 state enable	Create service vlan VLAN200
SW4(config-vlan)#exit	Exit VLAN configuration mode
SW4(config)#cvlan registration table map1 bridge 1	Create cvlan registration table map1
SW4(config-cvlan-registration)#cvlan 2 svlan 200	Map cvlan2 with svlan 200
SW4(config-cvlan-registration)#exit	Exit registration table
SW4(config)#interface eth1	Enter interface configuration mode for eth1
SW4(config-if)#switchport	Configure switchport
SW4(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW4(config-if)#witchport mode customer-edge hybrid	Configure switchport mode customer edge
SW4(config-if)#switchport customer-edge access vlan 2	Associate customer vlan2 with interface
SW4(config-if)#switchport customer-edge vlan registration map1	Attach registration table map1 with interface
SW4(config-if)#exit	Exit interface mode
SW4(config-if)#interface eth2	Enter interface configuration mode for eth2
SW4(config-if)#switchport	Make interface as switchport
SW4(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW4(config-if)#switchport mode provider-network	Configure switchport pnp port
SW4(config-if)#switchport provider-network allowed vlan all	Associate all svlan to the port
SW4(config-if)#interface eth3	Enter interface configuration mode for eth2
SW4(config-if)#switchport	Make interface as switchport
SW4(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW4(config-if)#switchport mode provider-network	Configure switchport pnp port

SW4(config-if)#switchport provider-network allowed vlan all	Associate all svlan to the port
SW4(config-if)#commit	Commit the configuration.
SW4(config-if)#exit	Exit interface configuration mode

Validation

```
SW4#sh br
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be affected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1          2     200           eth1        0000.0000.0a00    1     300
 1          2     200           eth2        0001.0000.0b00    1     300

SW1#sh br
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be affected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1          2     200           eth1        0000.0000.0b00    1     300
 1          2     200           eth3        0001.0000.0a00    1     300

SW1#sh cvlan registration table
Bridge          Table Name       Port List

======          ==========       =========

1               map1             eth1

CVLAN ID        SVLAN ID
========        ========
2               200
```

Layer 2 Protocol Tunneling (L2PT/L2CP Tunneling)

L2CP tunneling provides support for tunneling Control plane frames between CE nodes.

When control frames received at CEP port of PE bridge, predefined multicast address (01-00-C2-CD-CD-D0) is used for tunneling the packets across service provider network. If control packets are customer vlan tagged or untagged, then PE bridge will append corresponding service vlan tag to the control packet as per registration table / vlan translation table mapped to the port and send it across the service provider as a data packet.

When tunneled control packet with multicast address (01-00-C2-CD-CD-D0) received on PNP port, the multicast address is replaced with corresponding control packet multicast address and cvlan/svlan removal or updating is done as per registration table / vlan translation table.

Topology

Figure 2-6 displays a sample Provider Bridged topology with customer equipment.

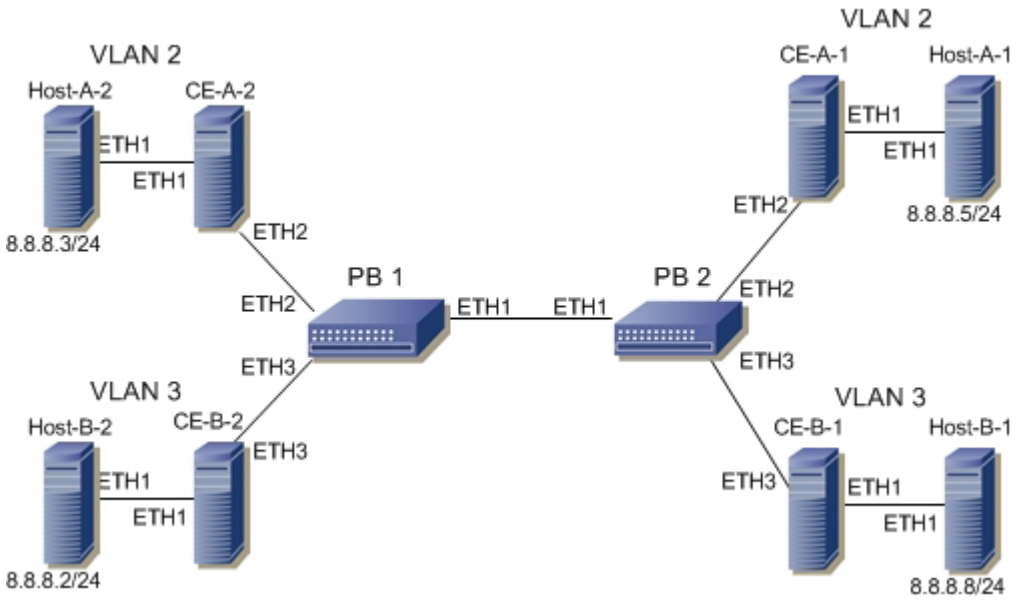


Figure 2-6: Provider Bridging with Customer Equipment Topology

Configuring the L2PT Protocol on the Interface

The following L2PT protocols are supported:

- EFM: Ethernet first mile (Link OAM)
- ELMI: Ethernet Local Management Interface
- LACP: Link Aggregation Control Protocol
- LLDP: Link Layer Discovery Protocol
- STP: Spanning Tree Protocols

PB1

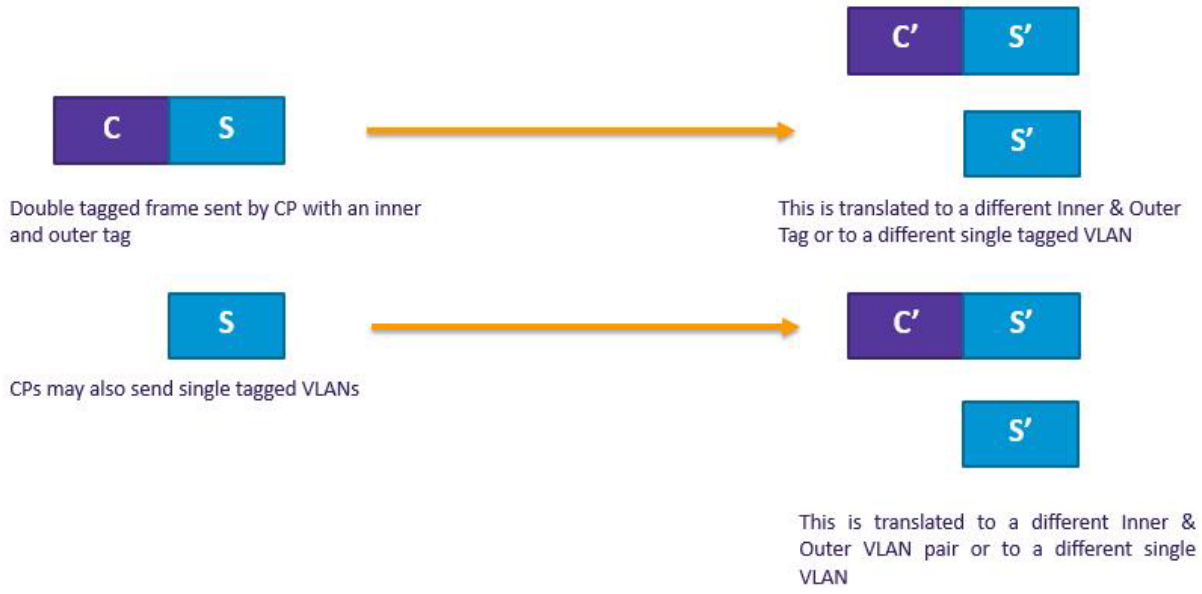
`PB1#configure terminal`	Enter Configure mode.
`PB1(config)#interface eth2`	Enter Interface mode
`PB1(config-if)#l2protocol stp peer`	Configure STP protocol as peer
`PB1(config-if)#l2protocol elmi tunnel`	Configure Elmi protocol as tunnel
`PB1(config-if)#l2protocol lldp tunnel`	Configure LLDP protocol as tunnel
`PB1(config-if)#l2protocol lacp discard`	Configure LACP protocol as discard
`PB1(config-if)#l2protocol efm discard`	Configure EFM protocol as discard
`PB1(config-if)#commit`	Commit the configuration.
`PB1(config-if)#exit`	Exit of the interface

Validation

```
PB1#show l2protocol processing interface eth2
Bridge    Interface Name                  Protocol       Processing Status
======    ==============                  ========       =================
1         eth2                           stp            Peer
1         eth2                           gmrp           Peer
1         eth2                           gvrp           Peer
1         eth2                           mmrp           Peer
1         eth2                           mvrp           Peer
1         eth2                           lacp           Discard
1         eth2                           lldp           Tunnel
1         eth2                           efm            Discard
1         eth2                           elmi           Tunnel
1         eth2                            ptp           Peer
```

Provider Bridging with VLAN Translation

This is a sample configurations to verify functionality to support provider-bridging feature with extended SVLAN translation as below:



Topology

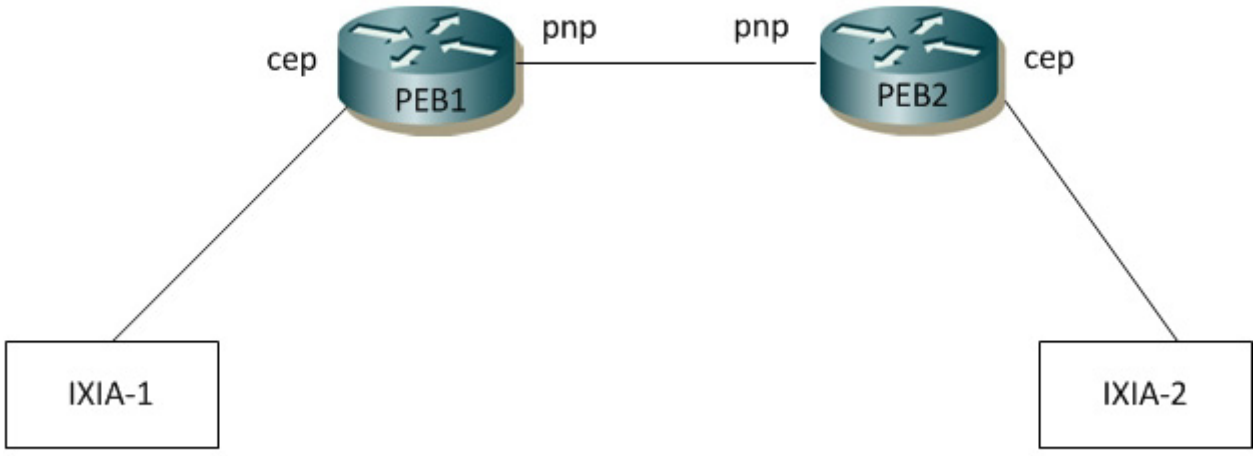


Figure 2-7: Provider Bridging with VLAN Traslation Topology

PEB1

Bridge Configuration

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol provider-rstp edge`	Enter Configure bridge type as provider-RSTP edge bridge
`(config)#commit`	Commit the configuration.
`(config)#exit`	Exit configure mode.

VLAN Configuration

`#configure terminal`	Enter configure mode.
`(config)#vlan database`	Enter VLAN database
`(config-vlan)# vlan 2-500 type customer bridge 1 state enable`	Configure customer VLANs on bridge 1
`(config-vlan)#vlan 2-1005 type service point-point bridge 1 state enable`	Configure service VLANs on bridge 1
`(config-vlan)#commit`	Commit the configuration.
`(config-vlan)#end`	Exit VLAN database and configure mode.

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 6`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 3 svlan 7`	Map CVLAN to SVLAN
`(config-cvlan-registration)#commit`	Commit the configuration.
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode customer-edge hybrid`	Configure port as customer-edge hybrid port
`(config-if)#switchport customer-edge hybrid allowed vlan all`	Add all VLANs configured above to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#commit`	Commit the configuration.
`(config-if)#end`	Exit interface and configure mode.

PNP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge9`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode provider-network`	Configure port as Provider Network Port (PNP)
`(config-if)#switchport provider-network allowed vlan all`	Add all VLANs configured above to this PNP port
`(config-if)#commit`	Commit the configuration.
`(config-if)#end`	Exit interface and configure mode.

PEB2

Bridge Configuration

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol provider-rstp edge`	Enter configure bridge type as provider-RSTP edge bridge
`(config-if)#commit`	Commit the configuration.
`(config)#exit`	Exit configure mode.

VLAN Configuration

`#configure terminal`	Enter configure mode.
`(config)#vlan database`	Enter VLAN database
`(config-vlan)#vlan 2-500 type customer bridge 1 state enable`	Configure customer VLANs on bridge 1
`(config-vlan)#vlan 501-1005 type service point-point bridge 1 state enable`	Configure service VLANs on bridge 1
`(config-if)#commit`	Commit the configuration.
`(config-vlan)#end`	Exit VLAN database and configure mode.

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 6`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 3 svlan 7`	Map CVLAN to SVLAN
`(config-cvlan-registration)#commit`	Commit the configuration.
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode customer-edge hybrid`	Configure port as customer-edge hybrid port
`(config-if)#switchport customer-edge hybrid allowed vlan all`	Add all VLANs configured above to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#commit`	Commit the configuration.
`(config-if)#end`	Exit interface and configure mode.

PNP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge9`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode provider-network`	Configure port as Provider Network Port (PNP)
`(config-if)#switchport provider-network allowed vlan all`	Add all VLANs configured above to this PNP port
`(config-if)#commit`	Commit the configuration.
`(config-if)#end`	Exit interface and configure mode.

Translation Cases

Case1 - (C S - C' S')

Configuration on PEB2

`#configure terminal`	Enter configure mode.
`(config)#interface ge9`	Enter the interface mode
`(config-if)#switchport provider-network vlan translation cvlan 2 svlan 6 cvlan 3 svlan 7`	Translate CVLAN and SVLAN to new CVLAN and new SVLAN on PNP port

Validation for Case 1

When tagged traffic with CVLAN 2 is sent from IXIA-1 to IXIA-2 with both CTAG and STAG entering provider network and gets translated to new CVLAN and SVLAN as per Case1.

```
PEB2#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address      FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
```

```
1                1            ge27        1402.ec1c.3144    1     300
1                6            ge9         6400.6a1e.d9a5    1     300
1          3     7            ge9         0000.0500.0400    1     300
1                7            ge9         6400.6a1e.d9a5    1     300
```

New SVLAN 7 is observed on PEB2 after translation. Also, captured packets on CEP show new CVLAN 3.

When tagged traffic for CVLAN 3 is sent from IXIA-2 to IXIA-1

```
PEB1#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+------------------+-----+---------+
 1                1             ge9          74e6.e2af.598b    1     300
 1          2     6             ge3          0000.0500.0400    1     300
 1          2     6             ge9          0000.0500.0700    1     300
```

When traffic is reversed and traffic has both new CVLAN 3 and SVLAN 7 on provider network from IXIA-2, translation to old CVLAN 2 and SVLAN 6 happens. Also, captured packets have CVLAN as 2.

Case2 - (C S - S')

Configuration on PEB2

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 6`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 3 svlan 7 untagged-pep`	Map CVLAN to SVLAN
`(config-cvlan-registration)#commit`	Commit the configuration.
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode
`(config-if)#switchport customer-edge hybrid vlan 3`	Allow access VLAN 3 configured above to this CEP port
`(config-if)#switchport customer-edge hybrid allowed vlan add 2-3`	Allow other VLANs configured to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#commit`	Commit the configuration.
`(config-if)#end`	Exit interface and configure mode.

PNP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge9`	Enter the interface mode

`(config-if)#no switchport provider-network vlan translation cvlan 2 svlan 6`	Unconfigure Translation Case1 from PNP port
`(config-if)#switchport provider-network vlan translation cvlan 2 svlan 6 svlan 7`	Configure Translation Case2 on PNP port
`(config-if)#commit`	Commit the configuration.
`(config-if)#end`	Exit interface and configure mode.

Validation for Case 2

When tagged traffic with CVLAN 2 is sent from IXIA-1 to IXIA-2 with both CTAG and STAG entering provider network and translated to new SVLAN as per Case2.

```
PEB2#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 --------+------+------+------+-----------+------------------+-----+---------+
 1                 1             ge27         1402.ec1c.3144    1     300
 1                 7             ge9          0000.0500.0400    1     300
```

New SVLAN 7 is observed on PEB2 after translation. At CEP port connected to IXIA-2, untagged traffic should be received.

When tagged traffic for CVLAN 3 is sent from IXIA-2 to IXIA-1.

```
PEB1#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 --------+------+------+------+-----------+------------------+-----+---------+
 1                 1             ge9          74e6.e2af.598b    1     300
 1         2       6             ge3          0000.0500.0400    1     300
 1         2       6             ge9          0000.0500.0700    1     300
```

When traffic is reversed and traffic has both new CVLAN 3 and SVLAN 7 from IXIA-2, translatiom to old CVLAN 2 and SVLAN 6 happens. Also, captured packets have CVLAN as 2.

Case3 - (S - S')

Configuration on PEB1

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 6`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 3 svlan 7`	Map CVLAN to SVLAN
`(config-cvlan-registration)#commit`	Commit the configuration.
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode

(config-if)#switchport customer-edge hybrid vlan 2	Allow access VLAN 2 configured above to this CEP port
(config-if)#switchport customer-edge hybrid allowed vlan add 2-3	Allow other VLANs configured to this CEP port
(config-if)#switchport customer-edge vlan registration map1	Attach the Map1 to CEP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

Configuration on PEB2

CEP Port Configuration (should be configured as PNP in this case)

#configure terminal	Enter configure mode.
(config)#interface ge3	Enter the interface mode
(config-if)#switchport	Configure switchport
(config-if)#switchport mode provider-network	Configure port as Provider Network Port (PNP)
(config-if)#switchport provider-network allowed vlan all	Add all VLANs configured above to this PNP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

PNP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface ge9	Enter the interface mode
(config-if)#no switchport provider-network vlan translation cvlan 2 svlan 6	Unconfigure Translation Case2 from PNP port
(config-if)#switchport provider-network vlan translation svlan 6 svlan 7	Configure Translation Case3 on PNP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

Validation for Case 3

When tagged traffic with CVLAN 2 is sent from IXIA-1 to IXIA-2 with only STAG entering provider network and translation happens to new SVLAN as per Case3.

```
PEB2#show bridge
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+------------------+-----+---------+
 1               1             ge27        1402.ec1c.3144    1     300
 1         2     6             ge9         0000.0500.0400    1     300
 1               6             ge9         6400.6a1e.d9a5    1     300
```

New SVLAN 7 is observed on PEB2 At PNP port connected to IXIA-2.

When double tagged traffic of CVLAN 2 and SVLAN 7 is sent from IXIA-2 to IXIA-1:

```
PEB1#show bridge
```

```
Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 --------+------+------+------+-----------+-----------------+-----+---------+
 1               1             ge9         74e6.e2af.598b    1     300
 1         3     7             ge3         0000.0500.0400    1     300
 1               6             ge9         0000.0500.0700    1     300
```

Here we get a tagged traffic of CVALN 2 when the captured at IXIA-1.

Case4 - (S - C' S')

Configuration on PEB1

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 6 untagged-pep`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 3 svlan 7`	Map CVLAN to SVLAN
`(config-cvlan-registration)#commit`	Commit the configuration.
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode
`(config-if)#switchport customer-edge hybrid vlan 2`	Allow access VLAN 2 configured above to this CEP port
`(config-if)#switchport customer-edge hybrid allowed vlan add 2-3`	Allow other VLANs configured to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#commit`	Commit the configuration.
`(config-if)#end`	Exit interface and configure mode.

Configuration on PEB2

CEP Port Configuration (should be configured as PNP in this case)

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode provider-network`	Configure port as Provider Network Port (PNP)
`(config-if)#switchport provider-network allowed vlan all`	Add all VLANs configured above to this PNP port

(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

PNP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface ge9	Enter the interface mode
(config-if)#no switchport provider-network vlan translation svlan 6	Unconfigure Translation Case2 from PNP port
(config-if)#switchport provider-network vlan translation svlan 6 cvlan 3 svlan 7	Configure Translation Case3 on PNP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

Validation for Case 4

When tagged traffic with CVLAN 2 is sent from IXIA-1 to IXIA-2 enters provider network and translation happens to new CVLAN and new SVLAN as per Case4.

```
PEB2#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+------------------+-----+---------+
 1               1             ge27         1402.ec1c.3144     1     300
 1         2     6             ge9          0000.0500.0400     1     300
 1               6             ge9          6400.6a1e.d9a5     1     300
```

When you observe the traffic received in IXIA-2, you can observe that new CVLAN 3 and SVLAN 7 tags can be seen. Here the VLAN 2 will be a data packet.

When tagged traffic for CVLAN 3 and SVLAN 7 is sent from IXIA-2 to IXIA-1:

```
PEB1#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+------------------+-----+---------+
 1               6             ge3          0000.0500.0400     1     300
 1               7             ge9          0000.0500.0700     1     300
```

When you observe, in PEB1 the packets will be dropped at the CEP port since only a single S tagged packets is obtained in the PNP.

Case5 - (C - C' S')

Configuration on PEB1

CVLAN Registration Table Configuration

#configure terminal	Enter configure mode.
(config)#cvlan registration table map1 bridge 1	Configure CVLAN registration table as map1
(config-cvlan-registration)#cvlan 2 cvlan3 svlan 4	Map CVLAN to C'VLAN and SVLAN
(config-cvlan-registration)#cvlan 5 cvlan 6 svlan 7	Map CVLAN to C'VLAN and SVLAN

(config-cvlan-registration)#commit	Commit the configuration.
(config-cvlan-registration)#end	End the CVLAN registration mode

CEP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface ge3	Enter the interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode customer-edge hybrid	Configure port as customer-edge hybrid port
(config-if)#switchport customer-edge hybrid allowed vlan all	Allow other VLANs configured to this CEP port
(config-if)#switchport customer-edge vlan registration map1	Attach the Map1 to CEP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

Configuration on PEB2

CEP Port Configuration (should be configured as PNP in this case)

#configure terminal	Enter configure mode.
(config)#interface ge3	Enter the interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode provider-network	Configure port as Provider Network Port (PNP)
(config-if)#switchport provider-network allowed vlan all	Add all VLANs configured above to this PNP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

PNP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface ge9	Enter the interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode provider-network	Configure port as Provider Network Port (PNP)
(config-if)#switchport provider-network allowed vlan all	Add all VLANs configured above to this PNP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

Validation for Case 5

When tagged traffic with CVLAN 2 is sent from IXIA-1 to IXIA-2 with both CTAG and STAG entering provider network and gets translated to new CVLAN and SVLAN as per Case5.

```
PEB2#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 --------+------+------+------+-----------+------------------+-----+---------+
 1               1              ge27         1402.ec1c.3144     1     300
 1               4              ge9          0000.0500.0400     1     300
 1               7              ge9          6400.6a1e.d9a5     1     300
```

When the packet is captured at PNP port of PEB2 CVLAN of 3 and SVLAN of 4 is seen.

When tagged traffic for CVLAN 6 and SVLAN 7 is sent from IXIA-2 to IXIA-1:

```
PEB1#show bridge
Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 --------+------+------+------+-----------+------------------+-----+---------+
 1               1              ge9          74e6.e2af.598b     1     300
 1               4              ge3          0000.0500.0400     1     300
 1        6      7              ge9          0000.0500.0700     1     300
```

When traffic is reversed and traffic has both new CVLAN 6 and SVLAN 7 on provider network from IXIA-2, translation to CVLAN 5 and SVLAN 7 happens. Also, captured packets have CVLAN as 2 based on the entry in the cvlan registration table.

Switchport ethertype

Bridge Configuration (for 0x88a8)

Configuration on PEB1

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 4`	Map CVLAN to SVLAN
`(config-cvlan-registration)#cvlan 3 svlan 6`	Map CVLAN to SVLAN
`(config-cvlan-registration)#commit`	Commit the configuration.
`(config-cvlan-registration)#end`	End the CVLAN registration mode

Configuration on PEB2

CEP Port Configuration (should be configured as PNP in this case)

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge3`	Enter the interface mode
`(config-if)#switchport`	Configure switchport

(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode provider-network	Configure port as Provider Network Port (PNP)
(config-if)#switchport provider-network allowed vlan all	Add all VLANs configured above to this PNP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

PNP Port Configuration

#configure terminal	Enter configure mode.
(config)#interface ge9	Enter the interface mode
(config-if)#switchport	Configure switchport
(config-if)#bridge-group 1	Attach port to bridge
(config-if)#switchport mode provider-network	Configure port as Provider Network Port (PNP)
(config-if)#switchport provider-network allowed vlan all	Add all VLANs configured above to this PNP port
(config-if)#dot1ad ethertype 0x88a8	Change the TPID of the SVLAN to 0x88a8
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

Validation for Switchport ethertype

To validate, send tagged traffic of VLAN 2 from IXIA-1.

Now at eth9 of PB2, capture the packets through IXIA-2 and verify that the traffic is received with double tag.

If the 2 tags CVLAN tag 2 will have the TPID of 0x8100 and SVLAN tag 4 will have a TPID of 0x88a8.

Provider Bridging QoS Configuration

This chapter contains sample provider bridging configurations for QoS.

Scenario: 1 Traffic flow from CEP to PNP

Topology

Figure 2-8: Provider Bridging with QoS Topology

Bridge Configuration

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol provider-rstp edge`	Enter configure bridge type as provider-RSTP edge bridge
`(config)#commit`	Commit the configuration.
`(config)#exit`	Exit configure mode.

VLAN Configuration

`#configure terminal`	Enter configure mode.
`(config)#vlan database`	Enter VLAN database
`(config-vlan)#vlan 2-500 type customer bridge 1 state enable`	Configure customer VLANs on bridge 1
`(config-vlan)#vlan 501-1005 type service point-point bridge 1 state enable`	Configure service VLANs on bridge 1
`(config-vlan)#commit`	Commit the configuration.
`(config-vlan)#end`	Exit VLAN database and configure mode.

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#cvlan 2 svlan 501`	Map CVLAN to SVLAN
`(config-cvlan-registration)#commit`	Commit the configuration.
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface xe2`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode customer-edge hybrid`	Configure port as customer-edge hybrid port
`(config-if)#switchport customer-edge hybrid allowed vlan all`	Add all VLANs configured above to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#commit`	Commit the configuration.
`(config-if)#end`	Exit interface and configure mode.

PNP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface xe3`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode provider-network`	Configure port as Provider Network Port (PNP)
`(config-if)#switchport provider-network allowed vlan add 501`	Add all VLANs configured above to this PNP port
`(config-if)#commit`	Commit the configuration.
`(config-if)#end`	Exit interface and configure mode.

QoS Configurations

`#configure terminal`	Enter configure mode.
`(config)#hardware-profile filter qos-ext enable`	Enabling Ingress extended QoS group for QoS support with statistics
`(config-if)#qos enable`	Enabling QoS
`(config-if)#qos statistics`	Enabling QoS statistics
`(config-if)#qos profile cos-to-queue cosq-cust1`	Configure QoS map profile
`config-ingress-cos-map)#cos 0 queue 1`	Configuring the cos value to be mapped to queue
`(config-ingress-cos-map)#exit`	Exit configure mode.
`(config)#qos profile queue-color-to-cos cosq-service1`	Configuring profile for queue color to cos map
`(config-egress-cos-map)#queue 1 cos 3`	Configuring the queue value to be cos remarked.
`(config-egress-cos-map)#exit`	Exit configure mode
`(config)#cvlan registration table map1 bridge 1`	Enter CVLAN registration mode

(config-cvlan-registration)#cvlan 2 svlan 501 cos-to-queue cosq-cust1	Map CVLAN to SVLAN with QoS map profile. Eg: when vlan 2 customer traffic with cos 0 value is received, queue will be assigned to 1 based on mapping.
(config-cvlan-registration)#end	End the CVLAN registration mode
(config)#interface xe3	Enter the interface mode
(config-if)#qos map-profile queue-color-to-cos cosq-service1	Map the profile to the PNP port. Eg: when traffic goes out of queue 1, cos value on service vlan header will be modified to 3 as remarking is enabled on the interface.
(config-if)#qos remark cos enable	Enabling Cos Remark on the Network Interface.
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode.

Validation for Scenario 1

```
#show cvlan registration table map1
Bridge          Table Name       Port List
======          ==========       =========
1               map1             xe2

CVLAN ID        T-CVLAN ID      SVLAN ID        Profile Name    Egress remark-
Cos
========        ==========      ========        ============
==================
2               -               501             cosq-cust1      No

#show qos-profile interface xe2
profile name: default
 profile type: cos-to-queue (Ingress)
 mapping:
 ---------------+----------------- | ---------------+-----------------
      INPUT     |     OUTPUT       |      INPUT     |     OUTPUT
 ---------------+----------------- | ---------------+-----------------
   COS  |  DEI  | Queue |  Color   |   COS  |  DEI  | Queue |  Color
 -------+-------+-------+--------- | -------+-------+-------+---------
  0       0       0       green    |  0       1       0       yellow
  1       0       1       green    |  1       1       1       yellow
  2       0       2       green    |  2       1       2       yellow
  3       0       3       green    |  3       1       3       yellow
  4       0       4       green    |  4       1       4       yellow
  5       0       5       green    |  5       1       5       yellow
  6       0       6       green    |  6       1       6       yellow
  7       0       7       green    |  7       1       7       yellow

profile name: default
 profile type: queue-color-to-cos (Egress)
 Status: Inactive
mapping:
 ----------------+-------- | ----------------+-------- | ----------------+----
----
      INPUT      | OUTPUT  |      INPUT      | OUTPUT  |      INPUT      |
OUTPUT
 ----------------+-------- | ----------------+-------- | ----------------+----
----
  Queue | Color  | COS     |  Queue | Color  | COS     |  Queue | Color  | COS
```

```
 -------+--------+-------- | -------+--------+-------- | -------+--------+----
----
  0       green    0       |  0       yellow   0       |  0       red      0
  1       green    1       |  1       yellow   1       |  1       red      1
  2       green    2       |  2       yellow   2       |  2       red      2
  3       green    3       |  3       yellow   3       |  3       red      3
  4       green    4       |  4       yellow   4       |  4       red      4
  5       green    5       |  5       yellow   5       |  5       red      5
  6       green    6       |  6       yellow   6       |  6       red      6
  7       green    7       |  7       yellow   7       |  7       red      7

#show qos-profile interface xe3
profile name: default
 profile type: cos-to-queue (Ingress)
 mapping:
 ---------------+----------------- | ---------------+-----------------
      INPUT     |     OUTPUT       |      INPUT     |     OUTPUT
 ---------------+----------------- | ---------------+-----------------
   COS  |  DEI  | Queue |  Color   |   COS  |  DEI  | Queue |  Color
 -------+-------+-------+--------- | -------+-------+-------+---------
  0       0       0       green    |  0       1       0       yellow
  1       0       1       green    |  1       1       1       yellow
  2       0       2       green    |  2       1       2       yellow
  3       0       3       green    |  3       1       3       yellow
  4       0       4       green    |  4       1       4       yellow
  5       0       5       green    |  5       1       5       yellow
  6       0       6       green    |  6       1       6       yellow
  7       0       7       green    |  7       1       7       yellow

profile name: cosq-service1
 profile type: queue-color-to-cos (Egress)
 Status: Active
mapping:
 ---------------+-------- | ---------------+-------- | ---------------+----
----
      INPUT      | OUTPUT  |      INPUT     | OUTPUT  |      INPUT     |
OUTPUT
 ---------------+-------- | ---------------+-------- | ---------------+----
----
  Queue | Color  | COS     |  Queue | Color  | COS     |  Queue | Color  | COS
 -------+--------+-------- | -------+--------+-------- | -------+--------+----
----
  0       green    0       |  0       yellow   0       |  0       red      0
  1       green    3       |  1       yellow   3       |  1       red      3
  2       green    2       |  2       yellow   2       |  2       red      2
  3       green    3       |  3       yellow   3       |  3       red      3
  4       green    4       |  4       yellow   4       |  4       red      4
  5       green    5       |  5       yellow   5       |  5       red      5
  6       green    6       |  6       yellow   6       |  6       red      6
  7       green    7       |  7       yellow   7       |  7       red      7
```

Scenario: 2 Traffic flow from PNP to CEP

Topology

Figure 2-9: Provider Bridging with QoS Topology

Bridge Configuration

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol provider-rstp edge`	Enter configure bridge type as provider-RSTP edge bridge
`(config)#commit`	Commit the configuration.
`(config)#exit`	Exit configure mode.

VLAN Configuration

`#configure terminal`	Enter configure mode.
`(config)#vlan database`	Enter VLAN database
`(config-vlan)#vlan 2-500 type customer bridge 1 state enable`	Configure customer VLANs on bridge 1
`(config-vlan)#vlan 501-1005 type service point-point bridge 1 state enable`	Configure service VLANs on bridge 1
`(config-vlan)#commit`	Commit the configuration.
`(config-vlan)#end`	Exit VLAN database and configure mode.

CVLAN Registration Table Configuration

`#configure terminal`	Enter configure mode.
`(config)#cvlan registration table map1 bridge 1`	Configure CVLAN registration table as map1
`(config-cvlan-registration)#commit`	Commit the configuration.
`(config-cvlan-registration)#end`	End the CVLAN registration mode

CEP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface xe2`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode customer-edge hybrid`	Configure port as customer-edge hybrid port
`(config-if)#switchport customer-edge hybrid allowed vlan all`	Add all VLANs configured above to this CEP port
`(config-if)#switchport customer-edge vlan registration map1`	Attach the Map1 to CEP port
`(config-if)#commit`	Commit the configuration.
`(config-if)#end`	Exit interface and configure mode.

PNP Port Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface xe3`	Enter the interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Attach port to bridge
`(config-if)#switchport mode provider-network`	Configure port as Provider Network Port (PNP)
`(config-if)#switchport provider-network allowed vlan add 501`	Add all VLANs configured above to this PNP port
`(config-if)#commit`	Commit the configuration.
`(config-if)#end`	Exit interface and configure mode.

QoS Configurations

`#configure terminal`	Enter configure mode.
`(config)#hardware-profile filter qos-ext enable`	Enabling Ingress extended QoS group for QoS support with statistics
`(config-if)#qos enable`	Enabling QoS
`(config-if)#qos statistics`	Enabling QoS statistics
`(config-if)#qos profile cos-to-queue cosq-cust1`	Configure QoS map profile
`config-ingress-cos-map)#cos 2 queue 5`	Configuring the cos value to be mapped to queue. Eg: when double tagged traffic with cos 2 for outer vlan is received, queue will be assigned to 5 based on mapping.
`(config-ingress-cos-map)#exit`	Exit configure mode.
`(config)#cvlan registration table map1 bridge 1`	Enter CVLAN registration mode
`(config-cvlan-registration)#cvlan 2 svlan 501 remark-cos`	Map CVLAN to SVLAN with remark cos enabled. Eg: when double tagged traffic with cos 2 for outer vlan is received, queue will be assigned to 5 based on mapping and cos value will be changed to 5 when it goes out of cep port since remark cos is enabled.

(config-cvlan-registration)#cvlan 3 svlan 501 remark-cos	Map CVLAN to SVLAN without remark cos. Eg: when double tagged traffic with cos 2 for outer vlan is received, and cos value will be forwarded as it is when it goes out of cep port since remark cos is not enabled for customer2.
(config-cvlan-registration)#end	End the CVLAN registration mode
(config)#configure terminal	Enter configure mode
(config)#interface xe3	Enter the interface mode
(config-if)#qos map-profile cos-to-queue cosq-service	Map the profile to the PNP port
(config-if)#commit	Commit the configuration.
(config-if)#end	Exit interface and configure mode

Validation for Scenario 2

```
#show cvlan registration table map1
Bridge          Table Name       Port List
======          ==========       =========
1               map1             xe2

CVLAN ID        T-CVLAN ID      SVLAN ID        Profile Name    Egress remark-
Cos
========        ==========      ========        ============
=================
2               -               501             N/A             Yes
3               -               501             N/A             No

#show qos-profile interface xe2
profile name: default
 profile type: cos-to-queue (Ingress)
 mapping:
 ---------------+----------------- | ---------------+-----------------
      INPUT     |     OUTPUT       |      INPUT     |     OUTPUT
 ---------------+----------------- | ---------------+-----------------
   COS  |  DEI  | Queue |  Color   |   COS  |  DEI  | Queue |  Color
 -------+-------+-------+--------- | -------+-------+-------+---------
  0       0       0       green    |  0       1       0       yellow
  1       0       1       green    |  1       1       1       yellow
  2       0       2       green    |  2       1       2       yellow
  3       0       3       green    |  3       1       3       yellow
  4       0       4       green    |  4       1       4       yellow
  5       0       5       green    |  5       1       5       yellow
  6       0       6       green    |  6       1       6       yellow
  7       0       7       green    |  7       1       7       yellow

profile name: default
 profile type: queue-color-to-cos (Egress)
 Status: Inactive
mapping:
 ----------------+-------- | ----------------+-------- | ----------------+----
----
      INPUT      | OUTPUT  |      INPUT      | OUTPUT  |      INPUT      |
OUTPUT
 ----------------+-------- | ----------------+-------- | ----------------+----
----
  Queue | Color  | COS     |  Queue | Color  | COS     |  Queue | Color  | COS
```

```
 -------+--------+-------- | -------+--------+-------- | -------+--------+----
----
  0       green    0       |  0       yellow   0       |  0       red      0
  1       green    1       |  1       yellow   1       |  1       red      1
  2       green    2       |  2       yellow   2       |  2       red      2
  3       green    3       |  3       yellow   3       |  3       red      3
  4       green    4       |  4       yellow   4       |  4       red      4
  5       green    5       |  5       yellow   5       |  5       red      5
  6       green    6       |  6       yellow   6       |  6       red      6
  7       green    7       |  7       yellow   7       |  7       red      7

#show qos-profile interface xe3
profile name: cosq-service
 profile type: cos-to-queue (Ingress)
 mapping:
 ---------------+----------------- | ---------------+-----------------
      INPUT     |     OUTPUT       |      INPUT     |     OUTPUT
 ---------------+----------------- | ---------------+-----------------
   COS  |  DEI  | Queue |  Color   |   COS  |  DEI  | Queue |  Color
 -------+-------+-------+--------- | -------+-------+-------+---------
  0       0       0       green    |  0       1       0       yellow
  1       0       1       green    |  1       1       1       yellow
  2       0       5       green    |  2       1       5       yellow
  3       0       3       green    |  3       1       3       yellow
  4       0       4       green    |  4       1       4       yellow
  5       0       5       green    |  5       1       5       yellow
  6       0       6       green    |  6       1       6       yellow
  7       0       7       green    |  7       1       7       yellow

profile name: default
 profile type: queue-color-to-cos (Egress)
 Status: Inactive
mapping:
 ---------------+-------- | ---------------+-------- | ---------------+----
----
      INPUT      | OUTPUT  |      INPUT     | OUTPUT  |      INPUT     |
OUTPUT
 ---------------+-------- | ---------------+-------- | ---------------+----
----
  Queue | Color  | COS     |  Queue | Color  | COS     |  Queue | Color  | COS
 -------+--------+-------- | -------+--------+-------- | -------+--------+----
----
  0       green    0       |  0       yellow   0       |  0       red      0
  1       green    1       |  1       yellow   1       |  1       red      1
  2       green    2       |  2       yellow   2       |  2       red      2
  3       green    3       |  3       yellow   3       |  3       red      3
  4       green    4       |  4       yellow   4       |  4       red      4
  5       green    5       |  5       yellow   5       |  5       red      5
  6       green    6       |  6       yellow   6       |  6       red      6
  7       green    7       |  7       yellow   7       |  7       red      7
```

Provider Bridging Untagged-pep Configuration

This is a sample configuration to verify functionality to support provider-bridging with untagged-pep feature.

For the below topology configuration,

1. While sending tagged traffic untagged-pep CVLAN 2, it should drop in provider edge bridge.
2. And while sending tagged traffic CVLAN 3 to the provider network, will egress with CVLAN 3 and SVLAN 12 tag and the same CVLAN and SVLAN tag from provider network, will egress with only CVLAN tag
3. And also for untagged traffic to the provider network, will egress with SVLAN 11 tag

Topology

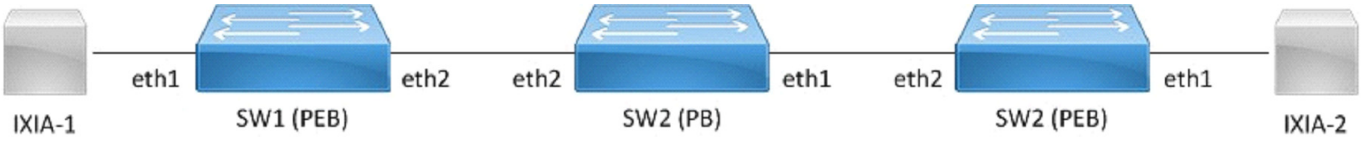


Figure 2-10: Provider bridging untagged-pep configuration

Configuration

SW1 (PEB)

`SW1#configure terminal`	Enter configuration mode
`SW1(config)#bridge 1 protocol provider-rstp edge`	Create bridge
`SW1(config)#vlan database`	Enter VLAN configuration mode
`SW1(config-vlan)#vlan 2-10 type customer bridge 1 state enable`	Create customer vlan VLAN 2-10
`SW1(config-vlan)#vlan 11-15 type service point-point bridge 1 state enable`	Create service vlan VLAN 11-15
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#cvlan registration table map1 bridge 1`	Create cvlan registration table map1
`SW1(config-cvlan-registration)#cvlan 2 svlan 11 untagged-pep`	Map cvlan2 with svlan 11
`SW1(config-cvlan-registration)#cvlan 3 svlan 12`	Map cvlan3 with svlan 12
`SW1(config-cvlan-registration)#cvlan 4 svlan 14`	Map cvlan4 with svlan 14
`SW1(config-cvlan-registration)#exit`	Exit registration table
`SW1(config)#interface eth1`	Enter interface configuration mode for eth1
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1

`SW1(config-if)#witchport mode customer-edge hybrid`	Configure switchport mode customer edge
`SW1(config-if)#switchport customer-edge hybrid vlan 2`	Associate customer vlan2 with interface
`SW1(config-if)#switchport customer-edge hybrid allowed vlan all`	Associate all customer vlan with interface
`SW1(config-if)#switchport customer-edge vlan registration map1`	Attach registration table map1 with interface
`SW1(config-if)#exit`	Exit interface mode
`SW1(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW1(config-if)#switchport`	Make interface as switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW1(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW1(config-if)#commit`	Apply the commit
`SW1(config-if)#exit`	Exit interface configuration mode
`SW1(config)#end`	Exit configuration mode

SW2 (PB)

`SW2#configure terminal`	Enter configuration mode
`SW2(config)#bridge 1 protocol provider-rstp`	Create provider bridge
`SW2(config)#vlan database`	Enter VLAN configuration mode
`SW2(config-vlan)# vlan 2-15 type service point-point bridge 1 state enable`	Create service vlan VLAN2-15
`SW2(config-vlan)#exit`	Exit VLAN configuration mode
`SW2(config)#interface eth1`	Enter interface configuration mode for eth1
`SW2(config-if)#switchport`	Make interface as switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW2(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW2(config-if)#exit`	Exit interface configuration mode
`SW2(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW2(config-if)#switchport`	Make interface as switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW2(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW2(config-if)#commit`	Apply the commit

SW2(config-if)#exit	Exit interface configuration mode
SW2(config)#end	Exit configuration mode

SW3 (PEB)

SW3#configure terminal	Enter configuration mode
SW3(config)#bridge 1 protocol provider-rstp edge	Create bridge
SW3(config)#vlan database	Enter VLAN configuration mode
SW3(config-vlan)#vlan 2-10 type customer bridge 1 state enable	Create customer vlan VLAN 2-10
SW3(config-vlan)#vlan 11-15 type service point-point bridge 1 state enable	Create service vlan VLAN11-15
SW3(config-vlan)#exit	Exit VLAN configuration mode
SW3(config)#cvlan registration table map1 bridge 1	Create cvlan registration table map1
SW3(config-cvlan-registration)#cvlan 2 svlan 11 untagged-pep	Map cvlan2 with svlan 200
SW3(config-cvlan-registration)#cvlan 3 svlan 12	Map cvlan3 with svlan 12
SW3(config-cvlan-registration)#cvlan 4 svlan 14	Map cvlan4 with svlan 14
SW3(config-cvlan-registration)#exit	Exit registration table
SW3(config)#interface eth1	Enter interface configuration mode for eth1
SW3(config-if)#switchport	Configure switchport
SW3(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW3(config-if)#witchport mode customer-edge hybrid	Configure switchport mode customer edge
SW3(config-if)#switchport customer-edge hybrid vlan 2	Associate customer vlan2 with interface
SW3(config-if)#switchport customer-edge hybrid allowed vlan all	Associate all customer vlan with interface
SW3(config-if)#switchport customer-edge vlan registration map1	Attach registration table map1 with interface
SW3(config-if)#exit	Exit interface mode
SW3(config-if)#interface eth2	Enter interface configuration mode for eth2
SW3(config-if)#switchport	Make interface as switchport
SW3(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW3(config-if)#switchport mode provider-network	Configure switchport pnp port
SW3(config-if)#switchport provider-network allowed vlan all	Associate all svlan to the port
SW3(config-if)#commit	Apply the commit
SW3(config-if)#exit	Exit interface configuration mode
SW3(config)#end	Exit configuration mode

Validation

```
SW3#sh bridge
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         4      14             eth1          0000.0100.0007    1     300

SW1#sh bridge
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1                14             eth1        0000.0100.0007    1     300

SW1#sh cvlan registration table map1
Bridge           Table Name       Port List

======           ==========       =========

1                map1             eth2

CVLAN ID         T-CVLAN ID       SVLAN ID         CCOS  SCOS  CCFI  SCFI
========         ==========       ========         ====  ====  ====  ====
3                -                12
2                -                11
4                -                14
```

CHAPTER 3 Provider Bridging Configuration (SVLAN)

This chapter contains sample provider bridging configurations for Customer-Network Port (CNP).

A provider bridged network is a virtual bridged Local Area Network that comprises provider bridges (SVLAN bridges and provider edge bridges) and attached LANs, under the administrative control of a single service provider. Provider bridges interconnect the separate MACs of the IEEE 802 LANs that compose a provider bridged network, relaying frames to provide connectivity between all the LANs that provide customer interfaces for each service instance.

Customer-Network Port (CNP)

In Q-in-Q, the customer network port is similar to provider network port, which can be present in provider-edge bridge (PEB) or provider bridge core (PB), where it can be directly connected to a dedicated customer network. Only SVLAN ids are configurable on Customer network port and learning and forwarding occurs based on SVLAN.

Note: Customer-Network Port is not supported in Qumran1 series platforms.

STAG-based Interface

In this case, the customer will be sending traffic with SVLAN, which will be learned and forwarded via provider network.

In this example, the xe1 interface allows S-TAG 100-200 and 400 traffic from customer.

```
(config)#interface xe1
(config-if)#switchport
(config-if)#dot1ad ethertype 0x88a8
(config-if)#bridge-group 1
(config-if)#switchport mode customer-network
(config-if)#switchport customer-network allowed vlan add 100-200,400
```

Port-based Interface

In this case, the customer traffic with C-VLAN/untagged, received on interface will be stacked with a customer-network SVLAN ID and will be forwarded via provider network. While egressing out of customer-network port for the default SVLAN, the outer SVLAN id will be stripped and the packet will be sent as C-TAG or untagged to customer device.

In this example, the xe1 interface allows C-TAG/untagged traffic from customers, adding an SVLAN ID 100 before forwarding to the provider network. While egressing out, the SVLAN ID100 will be stripped.

```
(config)#interface xe1
(config-if)#switchport
(config-if)#dot1ad ethertype 0x88a8
(config-if)#bridge-group 1
(config-if)#switchport mode customer-network
(config-if)#switchport customer-network allowed vlan add 100
(config-if)#switchport customer-network vlan 100
```

Topology

Figure 3-11: Single provider bridge configuration

Configuration

SW1 (PEB)

`SW1#configure terminal`	Enter configuration mode
`SW1(config)#bridge 1 protocol provider-rstp edge`	Create bridge
`SW1(config)#vlan database`	Enter VLAN configuration mode
`SW1(config-vlan)#vlan 100,200 type service point-point bridge 1 state enable`	Create service vlan VLAN 100, 200
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#interface eth1`	Enter interface configuration mode for eth1
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#dot1ad ethertype 0x88a8`	Add Provider Bridging Service VLAN tag identifier
`SW1(config-if)#switchport mode customer-network`	Configure switchport mode for CNP(customer network port)
`SW1(config-if)#switchport customer-network allowed vlan add 200`	Associate vlan 200 with interface
`SW1(config-if)#switchport customer-network vlan 200`	Add vlan 200 as default SVLAN-ID for traffic with CVLAN/ untagged
`SW1(config-if)#exit`	Exit interface mode
`SW1(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW1(config-if)#switchport`	Make interface as switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW1(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW1(config-if)#commit`	Commit the configuration.
`SW1(config-if)#exit`	Exit interface configuration mode

SW2 (PB)

`SW2#configure terminal`	Enter configuration mode
`SW2(config)#bridge 1 protocol provider-rstp`	Create provider bridge
`SW2(config)#vlan database`	Enter VLAN configuration mode
`SW2(config-vlan)#vlan 200 type service point-point bridge 1 state enable`	Create service vlan VLAN200
`SW2(config-vlan)#exit`	Exit VLAN configuration mode
`SW2(config)#interface eth1`	Enter interface configuration mode for eth1
`SW2(config-if)#switchport`	Make interface as switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW2(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW2(config-if)#exit`	Exit interface configuration mode
`SW2(config-if)#interface eth2`	Enter interface configuration mode for eth2
`SW2(config-if)#switchport`	Make interface as switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode provider-network`	Configure switchport pnp port
`SW2(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`SW2(config-if)#commit`	Commit the configuration.
`SW2(config-if)#exit`	Exit interface configuration mode

SW3 (PEB)

`SW3#configure terminal`	Enter configuration mode
`SW3(config)#bridge 1 protocol provider-rstp edge`	Create bridge
`SW3(config)#vlan database`	Enter VLAN configuration mode
`SW3(config-vlan)#vlan 200 type service point-point bridge 1 state enable`	Create service vlan VLAN200
`SW3(config-vlan)#exit`	Exit VLAN configuration mode
`SW3(config)#interface eth1`	Enter interface configuration mode for eth1
`SW3(config-if)#switchport`	Configure switchport
`SW3(config-if)#dot1ad ethertype 0x88a8`	Add Provider Bridging Service VLAN tag identifier
`SW3(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW3(config-if)#switchport mode customer-network`	Configure switchport CNP port
`SW3(config-if)#switchport customer-network allowed vlan add 200`	Associate vlan 200 with interface
`SW3(config-if)#switchport customer-network vlan 200`	Add vlan 200 as default SVLAN-ID for traffic with CVLAN/ untagged

SW3(config-if)#exit	Exit interface mode
SW3(config-if)#interface eth2	Enter interface configuration mode for eth2
SW3(config-if)#switchport	Make interface as switchport
SW3(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW3(config-if)#switchport mode provider-network	Configure switchport pnp port
SW3(config-if)#switchport provider-network allowed vlan all	Associate all svlan to the port
SW3(config-if)#commit	Commit the configuration.
SW3(config-if)#exit	Exit interface configuration mode

Validation

```
SW3#show bridge
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
Bridge    CVLAN  SVLAN  BVLAN     Port       MAC Address    FWD   Time-out
---------+------+------+------+-----------+-----------------+-----+------+
     1             200            eth1      0000.0000.0f00    1     300
     1             200            eth2      0001.0000.0800    1     300

SW1#show bridge
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
Bridge    CVLAN  SVLAN  BVLAN     Port       MAC Address    FWD   Time-out
---------+------+------+------+-----------+-----------------+-----+------+
     1             200            eth2      0000.0000.0f00    1     300
     1             200            eth1      0001.0000.0800    1     300
```

CHAPTER 4 Spanning Tree Protocol Configuration

This chapter contains a complete sample Spanning Tree Protocol (STP) configuration.

Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for Ethernet networks. The basic function of STP is to prevent bridge loops. Spanning tree also allows a network design to include redundant links to provide automatic backup paths if an active link fails, thus, eliminating the need to manually enable or disable the backup links.

Configurations

Topology

The following example is a simple multi-bridge topology.

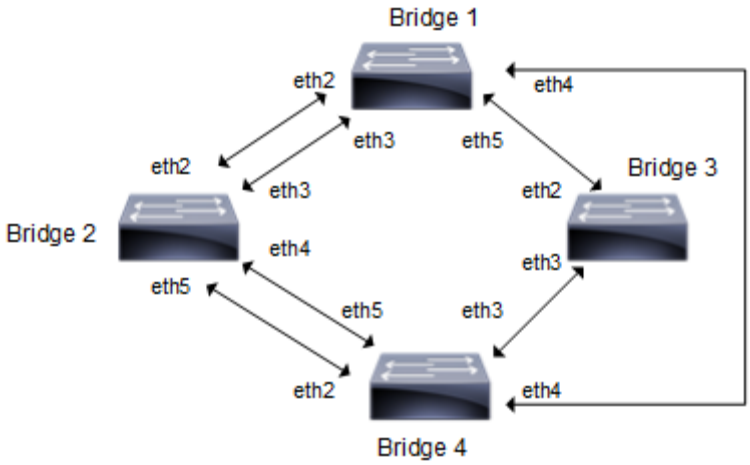


Figure 4-12: STP Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Bridge 1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#bridge 1 protocol ieee`	Add a bridge `(1)` to the spanning tree table
`Bridge1(config)#interface eth2`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth3`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.

`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth4`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth5`	Enter interface mode
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit interface mode.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol ieee`	Add a bridge (`2`) to the spanning tree table
`Bridge2(config)#interface eth2`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth3`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth4`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth5`	Enter interface mode
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-if)#exit`	Exit interface mode.

Bridge 4

`Bridge4#configure terminal`	Enter configure mode.
`Bridge4(config)#bridge 4 protocol ieee`	Add a bridge (`4`) to the spanning tree table
`Bridge4(config)#interface eth2`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth3`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth4`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth5`	Enter interface mode
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-if)#exit`	Exit interface mode.

Bridge 3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#bridge 3 protocol ieee`	Add a bridge `(3)` to the spanning tree table
`Bridge3(config)#interface eth2`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group `3`.
`Bridge3(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-if)#exit`	Exit interface mode.
`Bridge3(config)#interface eth3`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group `3`.

`Bridge3(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-if)#exit`	Exit interface mode.

Validation

Bridge 1

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 0
% 1: Root Id 80005254000be278
% 1: Bridge Id 80005254000be278
% 1: 15 topology changes - last topology change Sat Jul 10 09:44:56 2021
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - path cost 250 - designated cost 0
%   eth1: Designated Port Id 0x8003 - state Forwarding -Priority 128
%   eth1: Designated root 80005254000be278
%   eth1: Designated Bridge 80005254000be278
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Restricted-role OFF
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - path cost 250 - designated cost 0
%   eth2: Designated Port Id 0x8004 - state Forwarding -Priority 128
%   eth2: Designated root 80005254000be278
%   eth2: Designated Bridge 80005254000be278
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth2: forward-transitions 1
%   eth2: Restricted-role OFF
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - path cost 250 - designated cost 0
%   eth3: Designated Port Id 0x8005 - state Forwarding -Priority 128
%   eth3: Designated root 80005254000be278
%   eth3: Designated Bridge 80005254000be278
%   eth3: Message Age 0 - Max Age 20
```

```
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth3: forward-transitions 1
%   eth3: Restricted-role OFF
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - path cost 250 - designated cost 0
%   eth4: Designated Port Id 0x8006 - state Forwarding -Priority 128
%   eth4: Designated root 80005254000be278
%   eth4: Designated Bridge 80005254000be278
%   eth4: Message Age 0 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth4: forward-transitions 1
%   eth4: Restricted-role OFF
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Thu Jan  1 00:00:00 1970
% Default: 0 topology change(s)  - last topology change Thu Jan  1 00:00:00 1970


% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled

#show spanning-tree  interface eth1
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 0
% 1: Root Id 80005254000be278
% 1: Bridge Id 80005254000be278
% 1: 15 topology changes - last topology change Sat Jul 10 09:44:56 2021
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - path cost 250 - designated cost 0
%   eth1: Designated Port Id 0x8003 - state Forwarding -Priority 128
%   eth1: Designated root 80005254000be278
%   eth1: Designated Bridge 80005254000be278
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
```

```
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Restricted-role OFF
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
```

Bridge 2

```
#show spanning-tree
% 2: Bridge up - Spanning Tree Enabled
% 2: Root Path Cost 250 - Priority 32768
% 2: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 3
% 2: Root Id 80005254000be278
% 2: Bridge Id 8000525400b210cd
% 2: 5 topology changes - last topology change Sat Jul 10 09:44:30 2021
% 2: portfast bpdu-filter disabled
% 2: portfast bpdu-guard disabled
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - path cost 250 - designated cost 0
%   eth1: Designated Port Id 0x8003 - state Forwarding -Priority 128
%   eth1: Designated root 80005254000be278
%   eth1: Designated Bridge 80005254000be278
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 18 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Restricted-role OFF
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - path cost 250 - designated cost 0
%   eth2: Designated Port Id 0x8004 - state Blocked -Priority 128
%   eth2: Designated root 80005254000be278
%   eth2: Designated Bridge 80005254000be278
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 17 - Hello Timer 0 - topo change timer 0
%   eth2: forward-transitions 0
%   eth2: Restricted-role OFF
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - path cost 250 - designated cost
250
%   eth3: Designated Port Id 0x8005 - state Blocked -Priority 128
%   eth3: Designated root 80005254000be278
%   eth3: Designated Bridge 800052540047dc01
```

```
%   eth3: Message Age 3 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 13 - Hello Timer 0 - topo change timer 0
%   eth3: forward-transitions 1
%   eth3: Restricted-role OFF
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - path cost 250 - designated cost
250
%   eth4: Designated Port Id 0x8006 - state Blocked -Priority 128
%   eth4: Designated root 80005254000be278
%   eth4: Designated Bridge 800052540047dc01
%   eth4: Message Age 3 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 13 - Hello Timer 0 - topo change timer 0
%   eth4: forward-transitions 1
%   eth4: Restricted-role OFF
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Thu Jan  1 00:00:00 1970
% Default: 0 topology change(s)  - last topology change Thu Jan  1 00:00:00 1970


% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled

#show spanning-tree interface eth1
% 2: Bridge up - Spanning Tree Enabled
% 2: Root Path Cost 250 - Priority 32768
% 2: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 3
% 2: Root Id 80005254000be278
% 2: Bridge Id 8000525400b210cd
% 2: 5 topology changes - last topology change Sat Jul 10 09:44:30 2021
% 2: portfast bpdu-filter disabled
% 2: portfast bpdu-guard disabled
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - path cost 250 - designated cost 0
%   eth1: Designated Port Id 0x8003 - state Forwarding -Priority 128
%   eth1: Designated root 80005254000be278
%   eth1: Designated Bridge 80005254000be278
%   eth1: Message Age 0 - Max Age 20
```

```
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 17 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Restricted-role OFF
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
```

Bridge 3

```
#sho spanning-tree
% 3: Bridge up - Spanning Tree Enabled
% 3: Root Path Cost 250 - Priority 32768
% 3: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 3
% 3: Root Id 80005254000be278
% 3: Bridge Id 8000525400686eb9
% 3: 2 topology changes - last topology change Sat Jul 10 09:37:36 2021
% 3: portfast bpdu-filter disabled
% 3: portfast bpdu-guard disabled
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - path cost 250 - designated cost 0
%   eth1: Designated Port Id 0x8005 - state Forwarding -Priority 128
%   eth1: Designated root 80005254000be278
%   eth1: Designated Bridge 80005254000be278
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 18 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Restricted-role OFF
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - path cost 250 - designated cost
250
%   eth2: Designated Port Id 0x8004 - state Forwarding -Priority 128
%   eth2: Designated root 80005254000be278
%   eth2: Designated Bridge 8000525400686eb9
%   eth2: Message Age 1 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth2: forward-transitions 1
%   eth2: Restricted-role OFF
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%
% Default: Bridge up - Spanning Tree Enabled  - topology change detected
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
```

```
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Sat Jul 10 09:37:04 2021
% Default: 1 topology change(s)  - last topology change Sat Jul 10 09:37:04 2021


% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled

#  show spanning-tree interface eth1
% 3: Bridge up - Spanning Tree Enabled
% 3: Root Path Cost 250 - Priority 32768
% 3: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 3
% 3: Root Id 80005254000be278
% 3: Bridge Id 8000525400686eb9
% 3: 2 topology changes - last topology change Sat Jul 10 09:37:36 2021
% 3: portfast bpdu-filter disabled
% 3: portfast bpdu-guard disabled
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - path cost 250 - designated cost 0
%   eth1: Designated Port Id 0x8005 - state Forwarding -Priority 128
%   eth1: Designated root 80005254000be278
%   eth1: Designated Bridge 80005254000be278
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 17 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Restricted-role OFF
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
```

Bridge 4

```
#show spanning-tree
% 4: Bridge up - Spanning Tree Enabled
% 4: Root Path Cost 250 - Priority 32768
% 4: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 3
% 4: Root Id 80005254000be278
% 4: Bridge Id 800052540047dc01
% 4: 4 topology changes - last topology change Sat Jul 10 09:44:56 2021
% 4: portfast bpdu-filter disabled
% 4: portfast bpdu-guard disabled
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - path cost 250 - designated cost 0
%   eth1: Designated Port Id 0x8006 - state Forwarding -Priority 128
%   eth1: Designated root 80005254000be278
%   eth1: Designated Bridge 80005254000be278
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 17 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 1
```

```
%   eth1: Restricted-role OFF
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - path cost 250 - designated cost
250
%   eth2: Designated Port Id 0x8004 - state Forwarding -Priority 128
%   eth2: Designated root 80005254000be278
%   eth2: Designated Bridge 800052540047dc01
%   eth2: Message Age 1 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth2: forward-transitions 1
%   eth2: Restricted-role OFF
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - path cost 250 - designated cost
250
%   eth3: Designated Port Id 0x8005 - state Forwarding -Priority 128
%   eth3: Designated root 80005254000be278
%   eth3: Designated Bridge 800052540047dc01
%   eth3: Message Age 1 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth3: forward-transitions 1
%   eth3: Restricted-role OFF
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - path cost 250 - designated cost
250
%   eth4: Designated Port Id 0x8006 - state Forwarding -Priority 128
%   eth4: Designated root 80005254000be278
%   eth4: Designated Bridge 800052540047dc01
%   eth4: Message Age 1 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth4: forward-transitions 1
%   eth4: Restricted-role OFF
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%
```

```
#  show spanning-tree interface eth1
% 4: Bridge up - Spanning Tree Enabled
% 4: Root Path Cost 250 - Priority 32768
% 4: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 3
% 4: Root Id 80005254000be278
% 4: Bridge Id 800052540047dc01
% 4: 4 topology changes - last topology change Sat Jul 10 09:44:56 2021
% 4: portfast bpdu-filter disabled
% 4: portfast bpdu-guard disabled
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - path cost 250 - designated cost 0
%   eth1: Designated Port Id 0x8006 - state Forwarding -Priority 128
%   eth1: Designated root 80005254000be278
%   eth1: Designated Bridge 80005254000be278
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 18 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Restricted-role OFF
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%
%
```

CHAPTER 5 RSTP Configuration

This chapter contains a complete sample Rapid Spanning Tree Protocol (RSTP) configuration. RSTP provides rapid convergence of a spanning tree. It speeds up the reconfiguration of the tree after a change by using alternate ports.

Configuration

Topology

The following example is a simple multi-bridge topology.

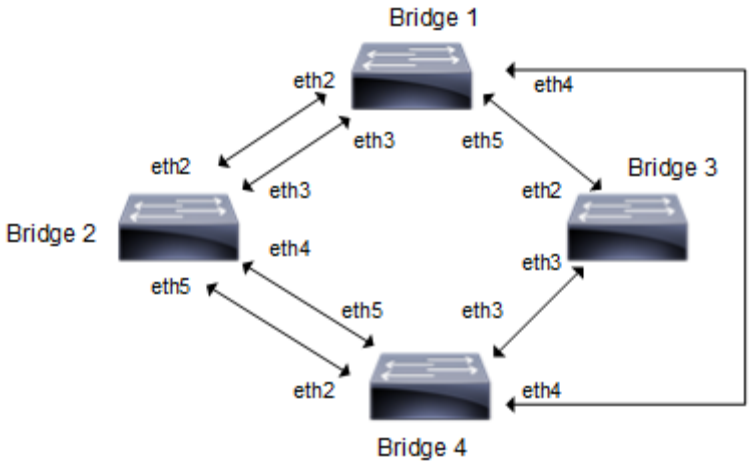


Figure 5-13: RSTP Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Bridge 1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#bridge 1 protocol rstp`	Add a bridge (`1`) to the rapid spanning tree table
`Bridge1(config)#interface eth2`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth3`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth4`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#exit`	Exit interface mode.

`Bridge1(config)#interface eth5`	Enter interface mode
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#commit`	Commit the configure on the node.
`Bridge1(config-if)#exit`	Exit interface mode.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol rstp`	Add a bridge (`2`) to the rapid spanning tree table
`Bridge2(config)#interface eth2`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth3`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth4`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth5`	Enter interface mode
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#commit`	Commit the configure on the node.
`Bridge2(config-if)#exit`	Exit interface mode.

Bridge 3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#bridge 3 protocol rstp`	Add a bridge `(3)` to the rapid spanning tree table
`Bridge3(config)#interface eth2`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group `3`.
`Bridge3(config-if)#exit`	Exit interface mode.
`Bridge3(config)#interface eth3`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group `3`.
`Bridge3(config-if)#commit`	Commit the configure on the node.
`Bridge3(config-if)#exit`	Exit interface mode.

Bridge 4

`Bridge4#configure terminal`	Enter configure mode.
`Bridge4(config)#bridge 4 protocol rstp`	Add a bridge `(4)` to the rapid spanning tree table
`Bridge4(config)#interface eth2`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth3`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth4`	Enter interface mode.
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth5`	Enter interface mode
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#commit`	Commit the configure on the node.
`Bridge4(config-if)#exit`	Exit interface mode.

Validation

show spanning-tree, show spanning-tree interface <if-name>

Bridge 1

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 200000 - Root Port 6 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 800052540046f549
% 1: Bridge Id 80005254009cb7e6
% 1: last topology change Tue Aug 11 02:25:01 2020
% 1: 30 topology change(s)  - last topology change Tue Aug 11 02:25:01 2020

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State
Discarding
%   eth2: Designated Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 800052540046f549
%   eth2: Designated Bridge 8000525400751db5
%   eth2: Message Age 1 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
```

```
%   eth2: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change
timer 0
%   eth2: forward-transitions 2
%   eth2: Restricted-role OFF
%   eth2: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State
Discarding
%   eth3: Designated Path Cost 200000
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 800052540046f549
%   eth3: Designated Bridge 8000525400751db5
%   eth3: Message Age 1 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change
timer 0
%   eth3: forward-transitions 3
%   eth3: Restricted-role OFF
%   eth3: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Rootport - State
Forwarding
%   eth4: Designated Path Cost 0
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth4: Designated Port Id 0x8006 - Priority 128  -
%   eth4: Root 800052540046f549
%   eth4: Designated Bridge 800052540046f549
%   eth4: Message Age 0 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change
timer 0
%   eth4: forward-transitions 6
%   eth4: Restricted-role OFF
%   eth4: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Alternate - State
Discarding
%   eth5: Designated Path Cost 200000
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 1
```

```
%   eth5: Designated Port Id 0x8004 - Priority 128  -
%   eth5: Root 800052540046f549
%   eth5: Designated Bridge 800052540065fd8c
%   eth5: Message Age 1 - Max Age 20
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change
timer 0
%   eth5: forward-transitions 4
%   eth5: Restricted-role OFF
%   eth5: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
%
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count
6
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Thu Jan  1 00:00:00 1970
% Default: 0 topology change(s)  - last topology change Thu Jan  1 00:00:00
1970

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
```

Bridge 2

```
#show spanning-tree
% 2: Bridge up - Spanning Tree Enabled  - topology change detected
% 2: Root Path Cost 200000 - Root Port 7 -  Bridge Priority 32768
% 2: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 2: Root Id 800052540046f549
% 2: Bridge Id 8000525400751db5
% 2: last topology change Tue Aug 11 02:25:00 2020
% 2: 22 topology change(s)  - last topology change Tue Aug 11 02:25:00 2020

% 2: portfast bpdu-filter disabled
% 2: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 800052540046f549
%   eth2: Designated Bridge 8000525400751db5
%   eth2: Message Age 1 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth2: forward-transitions 3
%   eth2: Restricted-role OFF
%   eth2: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
```

```
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
%   eth3: Designated Path Cost 200000
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 800052540046f549
%   eth3: Designated Bridge 8000525400751db5
%   eth3: Message Age 1 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth3: forward-transitions 3
%   eth3: Restricted-role OFF
%   eth3: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Alternate - State
Discarding
%   eth4: Designated Path Cost 0
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth4: Designated Port Id 0x8007 - Priority 128  -
%   eth4: Root 800052540046f549
%   eth4: Designated Bridge 800052540046f549
%   eth4: Message Age 0 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change
timer 0
%   eth4: forward-transitions 3
%   eth4: Restricted-role OFF
%   eth4: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Rootport - State
Forwarding
%   eth5: Designated Path Cost 0
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth5: Designated Port Id 0x8004 - Priority 128  -
%   eth5: Root 800052540046f549
%   eth5: Designated Bridge 800052540046f549
%   eth5: Message Age 0 - Max Age 20
%   eth5: Hello Time 2 - Forward Delay 15
```

```
%   eth5: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change
timer 0
%   eth5: forward-transitions 2
%   eth5: Restricted-role OFF
%   eth5: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
%
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count
6
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Thu Jan  1 00:00:00 1970
% Default: 0 topology change(s)  - last topology change Thu Jan  1 00:00:00
1970

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
```

Bridge 3

```
#show spanning-tree
% 3: Bridge up - Spanning Tree Enabled  - topology change detected
% 3: Root Path Cost 200000 - Root Port 5 -  Bridge Priority 32768
% 3: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 3: Root Id 800052540046f549
% 3: Bridge Id 800052540065fd8c
% 3: last topology change Tue Aug 11 02:25:00 2020
% 3: 16 topology change(s)  - last topology change Tue Aug 11 02:25:00 2020

% 3: portfast bpdu-filter disabled
% 3: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 800052540046f549
%   eth2: Designated Bridge 800052540065fd8c
%   eth2: Message Age 1 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
%   eth2: forward-transitions 2
%   eth2: Restricted-role OFF
%   eth2: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
```

```
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Rootport - State
Forwarding
%   eth3: Designated Path Cost 0
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 800052540046f549
%   eth3: Designated Bridge 800052540046f549
%   eth3: Message Age 0 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change
timer 0
%   eth3: forward-transitions 2
%   eth3: Restricted-role OFF
%   eth3: Version Rapid Spanning Tree Protocol - Receive RSTP - Send RSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count
6
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Thu Jan  1 00:00:00 1970
% Default: 0 topology change(s)  - last topology change Thu Jan  1 00:00:00
1970

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
```

Bridge 4

```
#show spanning-tree
% 4: Bridge up - Spanning Tree Enabled  - topology change detected
% 4: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 4: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 4: Root Id 800052540046f549
% 4: Bridge Id 800052540046f549
% 4: last topology change Tue Aug 11 02:24:58 2020
% 4: 6 topology change(s)  - last topology change Tue Aug 11 02:24:58 2020

% 4: portfast bpdu-filter disabled
% 4: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Path Cost 0
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 800052540046f549
%   eth2: Designated Bridge 800052540046f549
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth2: forward-transitions 1
```

```
%   eth2: Restricted-role OFF
%   eth2: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
%   eth3: Designated Path Cost 0
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 800052540046f549
%   eth3: Designated Bridge 800052540046f549
%   eth3: Message Age 0 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth3: forward-transitions 1
%   eth3: Restricted-role OFF
%   eth3: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
%   eth4: Designated Path Cost 0
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth4: Designated Port Id 0x8006 - Priority 128  -
%   eth4: Root 800052540046f549
%   eth4: Designated Bridge 800052540046f549
%   eth4: Message Age 0 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth4: forward-transitions 1
%   eth4: Restricted-role OFF
%   eth4: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Designated - State
Forwarding
%   eth5: Designated Path Cost 0
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth5: Designated Port Id 0x8007 - Priority 128  -
%   eth5: Root 800052540046f549
%   eth5: Designated Bridge 800052540046f549
```

```
%   eth5: Message Age 0 - Max Age 20
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth5: forward-transitions 1
%   eth5: Restricted-role OFF
%   eth5: Version Rapid Spanning Tree Protocol - Receive None - Send RSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
%
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count
6
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Thu Jan  1 00:00:00 1970
% Default: 0 topology change(s)  - last topology change Thu Jan  1 00:00:00
1970

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
```

CHAPTER 6 MSTP Configuration

This chapter contains a complete sample Multiple Spanning Tree Protocol (MSTP) configuration. MSTP allows multiple VLANs to be grouped into one spanning-tree instance. Every MST instance has a spanning-tree that is independent of other spanning-tree instances providing multiple forwarding paths for data traffic.

Configuration

Topology

This example gives a simple multi-bridge topology and its configuration.

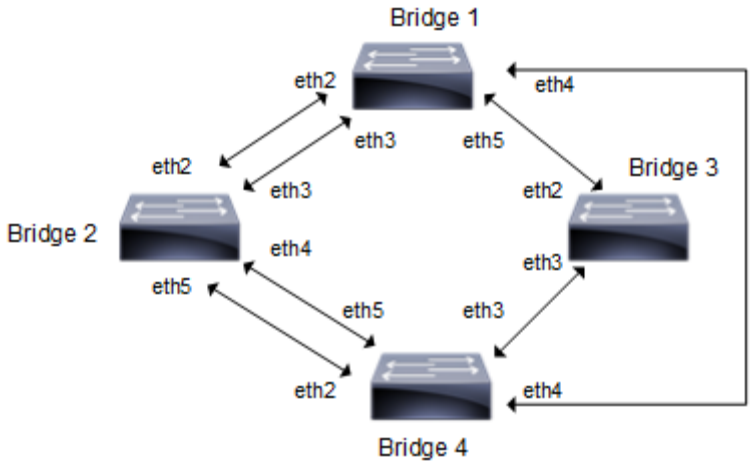


Figure 6-14: MSTP Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Bridge 1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#bridge 1 protocol mstp`	Add a bridge (1) to the multiple spanning tree table.
`Bridge1(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge1(config-vlan)#vlan 2 bridge 1 state enable`	Enable the state of VLAN 2 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 1.
`Bridge1(config-vlan)#vlan 3 bridge 1 state enable`	Enable the state of VLAN 3 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 1.
`Bridge1(config-vlan)#vlan 4 bridge 1 state enable`	Enable the state of VLAN 4 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 4 on bridge 1.
`Bridge1(config-vlan)#vlan 5 bridge 1 state enable`	Enable the state of VLAN 5 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 1.
`Bridge1(config-vlan)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge1(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree

`Bridge1(config-mst)#bridge 1 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge1(config-mst)#bridge 1 instance 3 vlan 3`	Create another instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge1(config-mst)#bridge 1 instance 4 vlan 4`	Create another instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge1(config-mst)#bridge 1 instance 5 vlan 5`	Create another instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge1(config-mst)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-mst)#exit`	Exit MST Configuration mode.
`Bridge1(config)#interface eth2`	Enter interface mode for eth2
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth3`	Enter interface mode for eth3.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth4`	Enter interface mode for eth4.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance

`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth5`	Enter interface mode for eth5.
`Bridge1(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit interface mode.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol mstp`	Add a bridge (2) to the multiple spanning
`Bridge2(config)#bridge 2 priority 4096`	Assign priority to this bridge.
`Bridge2(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge2(config-vlan)#vlan 2 bridge 2 state enable`	Enable the state of VLAN 2 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 2.
`Bridge2(config-vlan)#vlan 3 bridge 2 state enable`	Enable the state of VLAN 3 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 2
`Bridge2(config-vlan)#vlan 4 bridge 2 state enable`	Enable the state of VLAN 4 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 4 on bridge 2
`Bridge2(config-vlan)#vlan 5 bridge 2 state enable`	Enable the state of VLAN 5 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 2
`Bridge2(config-vlan)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge2(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree configuration mode
`Bridge2(config-mst)#bridge 2 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.

`Bridge2(config-mst)#bridge 2 instance 3 vlan 3`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge2(config-mst)#bridge 2 instance 4 vlan 4`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge2(config-mst)#bridge 2 instance 5 vlan 5`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge2(config-mst)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-mst)#exit`	Exit MST Configuration mode.
`Bridge2(config)#interface eth2`	Enter interface mode for eth2
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2
`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth3`	Enter interface mode for eth3
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2
`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3 priority 16`	Assign bridge-group 2 to this instance and set a port priority in order of 16 for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority.
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4 priority 16`	Assign bridge-group 2 to this instance and set a port priority in order of 16 for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#commit`	Commit the candidate configuration to the running configuration.

`Bridge2(config-if)#exit`	Exit interface mode
`Bridge2(config)#interface eth4`	Enter interface mode for eth4
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2
`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth5`	Enter interface mode for eth5
`Bridge2(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2
`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-if)#exit`	Exit interface mode.

Bridge 3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#bridge 3 protocol mstp`	Add a bridge (3) to the multiple spanning tree table
`Bridge3(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge3(config-vlan)#vlan 2 bridge 3 state enable`	Enable the state of VLAN 2 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 3.
`Bridge3(config-vlan)#vlan 3 bridge 3 state enable`	Enable the state of VLAN 3 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 3.
`Bridge3(config-vlan)#vlan 4 bridge 3 state enable`	Enable the state of VLAN 4 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 4 on bridge 3.

`Bridge3(config-vlan)#vlan 5 bridge 3 state enable`	Enable the state of VLAN 5 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 3.
`Bridge3(config-vlan)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge3(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree Configuration mode.
`Bridge3(config-mst)#bridge 3 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge3(config-mst)#bridge 3 instance 3 vlan 3`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge3(config-mst)#bridge 3 instance 4 vlan 4`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge3(config-mst)#bridge 3 instance 5 vlan 5`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge3(config-mst)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-mst)#exit`	Exit MST Configuration mode.
`Bridge3(config)#interface eth2`	Enter interface mode for eth2
`Bridge3(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge3(config-if)#bridge-group 3`	Associating the interface to bridge-group 3
`Bridge3(config-if)#bridge-group 3 instance 2`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 3`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 4`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 5`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-if)#exit`	Exit interface mode.
`Bridge3(config)#interface eth3`	Enter interface mode for eth3
`Bridge3(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge3(config-if)#bridge-group 3`	Associating the interface to bridge-group 3
`Bridge3(config-if)#bridge-group 3 instance 2`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 3`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 4`	Assigning bridge-group 3 to this instance

`Bridge3(config-if)#bridge-group 3 instance 5`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-if)#exit`	Exit interface mode.

Bridge 4

`Bridge4#configure terminal`	Enter configure mode.
`Bridge4(config)#bridge 4 protocol mstp`	Add a bridge (4) to the multiple spanning tree table
`Bridge4(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge4(config-vlan)#vlan 2 bridge 4 state enable`	Enable the state of VLAN 2 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 4.
`Bridge4(config-vlan)#vlan 3 bridge 4 state enable`	Enable the state of VLAN 3 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 4.
`Bridge4(config-vlan)#vlan 4 bridge 4 state enable`	Enable the state of VLAN 4 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 4 on bridge 4.
`Bridge4(config-vlan)#vlan 5 bridge 4 state enable`	Enable the state of VLAN 5 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 4.
`Bridge4(config-vlan)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge4(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree Configuration mode.
`Bridge4(config-mst)#bridge 4 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge4(config-mst)#bridge 4 instance 3 vlan 3`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge4(config-mst)#bridge 4 instance 4 vlan 4`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge4(config-mst)#bridge 4 instance 5 vlan 5`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge4(config-mst)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-mst)#exit`	Exit MST Configuration mode.
`Bridge4(config)#interface eth2`	Enter interface mode for eth2
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group  4`	Associating the interface to bridge-group 4
`Bridge4(config-if)#bridge-group 4 instance 2`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 3`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 4`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 5`	Assigning bridge-group 4 to this instance

`Bridge4(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth3`	Enter interface mode for eth3
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group  4`	Associating the interface to bridge-group 4
`Bridge4(config-if)#bridge-group 4 instance 2`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 3`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 4`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 5`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth4`	Enter interface mode for eth4
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group  4`	Associating the interface to bridge-group 4
`Bridge4(config-if)#bridge-group 4 instance 2`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 3`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 4`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 5`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth5`	Enter interface mode for eth5
`Bridge4(config-if)#switchport`	Configure interface as a layer 2 port.
`Bridge4(config-if)#bridge-group  4`	Associating the interface to bridge-group 4
`Bridge4(config-if)#bridge-group 4 instance 2`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 3`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 4`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#bridge-group 4 instance 5`	Assigning bridge-group 4 to this instance
`Bridge4(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge4(config-if)#exit`	Exit interface mode.

Validation

show spanning-tree, show spanning-tree mst detail

```
# show spanning-tree mst detail
```

```
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: CIST Root Path Cost 0 - CIST Root Port 4 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% 1: CIST Root Id 1000525400751db5
% 1: CIST Reg Root Id 1000525400751db5
% 1: CIST Bridge Id 80005254009cb7e6
% 1: 32 topology change(s)  - last topology change Mon Aug 17 10:45:25 2020

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Rootport - State
Forwarding
%   eth2: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth2: Designated Port Id 0x8004 - CIST Priority 128  -
%   eth2: CIST Root 1000525400751db5
%   eth2: Regional Root 1000525400751db5
%   eth2: Designated Bridge 1000525400751db5
%   eth2: Message Age 0 - Max Age 20
%   eth2: CIST Hello Time 2 - Forward Delay 15
%   eth2: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change
timer 0
%   eth2: forward-transitions 1
%   eth2: Restricted-role OFF
%   eth2: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State
Discarding
%   eth3: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth3: Designated Port Id 0x8005 - CIST Priority 128  -
%   eth3: CIST Root 1000525400751db5
%   eth3: Regional Root 1000525400751db5
%   eth3: Designated Bridge 1000525400751db5
%   eth3: Message Age 0 - Max Age 20
%   eth3: CIST Hello Time 2 - Forward Delay 15
%   eth3: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change
timer 0
%   eth3: forward-transitions 2
%   eth3: Restricted-role OFF
%   eth3: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Alternate - State
Discarding
%   eth4: Designated External Path Cost 0 -Internal Path Cost 200000
```

```
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth4: Designated Port Id 0x8006 - CIST Priority 128  -
%   eth4: CIST Root 1000525400751db5
%   eth4: Regional Root 1000525400751db5
%   eth4: Designated Bridge 800052540046f549
%   eth4: Message Age 0 - Max Age 20
%   eth4: CIST Hello Time 2 - Forward Delay 15
%   eth4: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change
timer 0
%   eth4: forward-transitions 3
%   eth4: Restricted-role OFF
%   eth4: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Designated - State
Forwarding
%   eth5: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth5: Designated Port Id 0x8007 - CIST Priority 128  -
%   eth5: CIST Root 1000525400751db5
%   eth5: Regional Root 1000525400751db5
%   eth5: Designated Bridge 80005254009cb7e6
%   eth5: Message Age 0 - Max Age 20
%   eth5: CIST Hello Time 2 - Forward Delay 15
%   eth5: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
%   eth5: forward-transitions 4
%   eth5: Restricted-role OFF
%   eth5: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
%

% Instance  2:  Vlans: 2

% 1: MSTI Root Path Cost 200000 -MSTI Root Port 6 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 800252540046f549
% 1: MSTI Bridge Id 80025254009cb7e6
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State
Discarding
%   eth2: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured CST External Path cost 200000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 800252540046f549
%   eth2: Designated Bridge 80025254009cb7e6
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
```

```
%   eth2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State
Discarding
%   eth3: Designated Internal Path Cost 200000  - Designated Port Id 0x8005
%   eth3: Configured Internal Path Cost 200000
%   eth3: Configured CST External Path cost 200000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 800252540046f549
%   eth3: Designated Bridge 80025254009cb7e6
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Rootport - State
Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 200000
%   eth4: Configured CST External Path cost 200000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 800252540046f549
%   eth4: Designated Bridge 80025254009cb7e6
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1

%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Alternate - State
Discarding
%   eth5: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth5: Configured Internal Path Cost 200000
%   eth5: Configured CST External Path cost 200000
%   eth5: CST Priority 128  - MSTI Priority 128
%   eth5: Designated Root 800252540046f549
%   eth5: Designated Bridge 80025254009cb7e6
%   eth5: Message Age 0
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1


% Instance  3:  Vlans: 3

% 1: MSTI Root Path Cost 200000 -MSTI Root Port 6 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 800352540046f549
% 1: MSTI Bridge Id 80035254009cb7e6
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State
Discarding
%   eth2: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured CST External Path cost 200000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 800352540046f549
%   eth2: Designated Bridge 80035254009cb7e6
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State
Discarding
```

```
%   eth3: Designated Internal Path Cost 200000  - Designated Port Id 0x1005
%   eth3: Configured Internal Path Cost 200000
%   eth3: Configured CST External Path cost 200000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 800352540046f549
%   eth3: Designated Bridge 80035254009cb7e6
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Rootport - State
Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 200000
%   eth4: Configured CST External Path cost 200000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 800352540046f549
%   eth4: Designated Bridge 80035254009cb7e6
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1

%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Alternate - State
Discarding
%   eth5: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth5: Configured Internal Path Cost 200000
%   eth5: Configured CST External Path cost 200000
%   eth5: CST Priority 128  - MSTI Priority 128
%   eth5: Designated Root 800352540046f549
%   eth5: Designated Bridge 80035254009cb7e6
%   eth5: Message Age 0
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1


% Instance  4:  Vlans: 4

% 1: MSTI Root Path Cost 200000 -MSTI Root Port 6 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 800452540046f549
% 1: MSTI Bridge Id 80045254009cb7e6
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State
Discarding
%   eth2: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured CST External Path cost 200000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 800452540046f549
%   eth2: Designated Bridge 80045254009cb7e6
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State
Discarding
%   eth3: Designated Internal Path Cost 200000  - Designated Port Id 0x1005
%   eth3: Configured Internal Path Cost 200000
%   eth3: Configured CST External Path cost 200000
```

```
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 800452540046f549
%   eth3: Designated Bridge 80045254009cb7e6
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Rootport - State
Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 200000
%   eth4: Configured CST External Path cost 200000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 800452540046f549
%   eth4: Designated Bridge 80045254009cb7e6
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1

%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Alternate - State
Discarding
%   eth5: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth5: Configured Internal Path Cost 200000
%   eth5: Configured CST External Path cost 200000
%   eth5: CST Priority 128  - MSTI Priority 128
%   eth5: Designated Root 800452540046f549
%   eth5: Designated Bridge 80045254009cb7e6
%   eth5: Message Age 0
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1


% Instance  5:  Vlans: 5

% 1: MSTI Root Path Cost 200000 -MSTI Root Port 6 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 800552540046f549
% 1: MSTI Bridge Id 80055254009cb7e6
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Alternate - State
Discarding
%   eth2: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured CST External Path cost 200000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 800552540046f549
%   eth2: Designated Bridge 80055254009cb7e6
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State
Discarding
%   eth3: Designated Internal Path Cost 200000  - Designated Port Id 0x8005
%   eth3: Configured Internal Path Cost 200000
%   eth3: Configured CST External Path cost 200000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 800552540046f549
%   eth3: Designated Bridge 80055254009cb7e6
```

```
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Rootport - State
Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 200000
%   eth4: Configured CST External Path cost 200000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 800552540046f549
%   eth4: Designated Bridge 80055254009cb7e6
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1

%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Alternate - State
Discarding
%   eth5: Designated Internal Path Cost 200000  - Designated Port Id 0x8004
%   eth5: Configured Internal Path Cost 200000
%   eth5: Configured CST External Path cost 200000
%   eth5: CST Priority 128  - MSTI Priority 128
%   eth5: Designated Root 800552540046f549
%   eth5: Designated Bridge 80055254009cb7e6
%   eth5: Message Age 0
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1

    #show spanning-tree
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: CIST Root Path Cost 0 - CIST Root Port 4 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% 1: CIST Root Id 1000525400751db5
% 1: CIST Reg Root Id 1000525400751db5
% 1: CIST Bridge Id 80005254009cb7e6
% 1: 32 topology change(s)  - last topology change Mon Aug 17 10:45:25 2020

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Rootport - State
Forwarding
%   eth2: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth2: Designated Port Id 0x8004 - CIST Priority 128  -
%   eth2: CIST Root 1000525400751db5
%   eth2: Regional Root 1000525400751db5
%   eth2: Designated Bridge 1000525400751db5
%   eth2: Message Age 0 - Max Age 20
%   eth2: CIST Hello Time 2 - Forward Delay 15
%   eth2: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change
timer 0
%   eth2: forward-transitions 1
%   eth2: Restricted-role OFF
%   eth2: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
```

```
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State
Discarding
%   eth3: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth3: Designated Port Id 0x8005 - CIST Priority 128  -
%   eth3: CIST Root 1000525400751db5
%   eth3: Regional Root 1000525400751db5
%   eth3: Designated Bridge 1000525400751db5
%   eth3: Message Age 0 - Max Age 20
%   eth3: CIST Hello Time 2 - Forward Delay 15
%   eth3: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change
timer 0
%   eth3: forward-transitions 2
%   eth3: Restricted-role OFF
%   eth3: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Alternate - State
Discarding
%   eth4: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth4: Designated Port Id 0x8006 - CIST Priority 128  -
%   eth4: CIST Root 1000525400751db5
%   eth4: Regional Root 1000525400751db5
%   eth4: Designated Bridge 800052540046f549
%   eth4: Message Age 0 - Max Age 20
%   eth4: CIST Hello Time 2 - Forward Delay 15
%   eth4: CIST Forward Timer 0 - Msg Age Timer 3 - Hello Timer 0 - topo change
timer 0
%   eth4: forward-transitions 3
%   eth4: Restricted-role OFF
%   eth4: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Designated - State
Forwarding
%   eth5: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth5: Designated Port Id 0x8007 - CIST Priority 128  -
%   eth5: CIST Root 1000525400751db5
%   eth5: Regional Root 1000525400751db5
%   eth5: Designated Bridge 80005254009cb7e6
%   eth5: Message Age 0 - Max Age 20
%   eth5: CIST Hello Time 2 - Forward Delay 15
```

```
%   eth5: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   eth5: forward-transitions 4
%   eth5: Restricted-role OFF
%   eth5: Version Multiple Spanning Tree Protocol - Receive MSTP - Send MSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
```

CHAPTER 7 Disable Spanning Tree Configuration

This chapter describes disabling spanning tree operation on a per Multiple Spanning Tree Instance (MSTI) basis.

Disabling MSTP Configuration

Topology

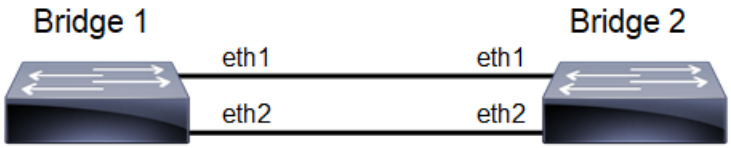


Figure 7-15: Disable Spanning Tree Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Bridge 1

Disabling MSTP per instance

`Bridge1(config-mst)#no bridge 1 instance 2`	Disable spanning tree for MSTP on instance 2
`Bridge1(config-mst)#no bridge 1 instance 3`	Disable spanning tree for MSTP on instance 3
`Bridge1(config-mst)#commit`	Commit the configure on the node.

Disabling MSTP globally

`Bridge1(config)#no bridge 1 multiple-spanning-tree enable bridge-forward`	Disable spanning tree globally for MSTP and keeping the ports in forwarding state.
`Bridge1(config)#commit`	Commit the configure on the node.

Disabling MSTP per port

`Bridge1(config)#interface ge2`	Enter interface mode for ge2.
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for MSTP and put port on forwarding state. This command disables any type of STP on the port.
`Bridge1(config-if)#commit`	Commit the configure on the node.

Bridge 2

Disabling MSTP per instance

`Bridge2(config-mst)#no bridge 1 instance 2`	Disable spanning tree for MSTP on instance 2
`Bridge2(config-mst)#no bridge 1 instance 3`	Disable spanning tree for MSTP on instance 3
`Bridge2(config-mst)#commit`	Commit the configure on the node.

Disabling MSTP globally

`Bridge2(config)#no bridge 1 multiple-spanning-tree enable bridge-forward`	Disable spanning tree globally for MSTP.
`Bridge2(config)#commit`	Commit the configure on the node.

Disabling MSTP per port

`Bridge2(config)#interface xe2`	Enter interface mode for xe2.
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for MSTP and put port on forwarding state. This command disables any type of STP on the port.
`Bridge2(config-if)#commit`	Commit the configure on the node.

Validation

Bridge 1

Verify MSTP details with the `show spanning-tree mst detail` command.

```
#show spanning-tree mst detail
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: CIST Root Path Cost 0 - CIST Root Port 905 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% 1: CIST Root Id 80003417ebfbe9c4
% 1: CIST Reg Root Id 80003417ebfbe9c4
% 1: CIST Bridge Id 800064006ac779a0
% 1: 9 topology change(s)  - last topology change Thu Nov 17 15:06:17 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport -
State Forwarding
%   ge2: Designated External Path Cost 0 -Internal Path Cost 20000
%   ge2: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge2: Designated Port Id 0x838a - CIST Priority 128  -
%   ge2: CIST Root 80003417ebfbe9c4
%   ge2: Regional Root 80003417ebfbe9c4
%   ge2: Designated Bridge 80003417ebfbe9c4
%   ge2: Message Age 0 - Max Age 20
%   ge2: CIST Hello Time 2 - Forward Delay 15
%   ge2: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change
timer 0
%   ge2: forward-transitions 1
%   ge2: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%   ge2: Configured Link Type point-to-point - Current point-to-point
%   ge2: No auto-edge configured - Current port Auto Edge off
%
```

```
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Alternate -
State Discarding
%   ge3: Designated External Path Cost 0 -Internal Path Cost 20000
%   ge3: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge3: Designated Port Id 0x838b - CIST Priority 128  -
%   ge3: CIST Root 80003417ebfbe9c4
%   ge3: Regional Root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: CIST Hello Time 2 - Forward Delay 15
%   ge3: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1 - topo change
timer 0
%   ge3: forward-transitions 2
%   ge3: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
%   ge3: Configured Link Type point-to-point - Current point-to-point
%   ge3: No auto-edge configured - Current port Auto Edge off

% Instance  2:  Vlans: 2

% 1: MSTI Root Path Cost 20000 -MSTI Root Port 5001 - MSTI Bridge Priority
32768
% 1: MSTI Root Id 80023417ebfbe9c4
% 1: MSTI Bridge Id 800264006ac779a0
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport -
State Forwarding
%   ge2: Designated Internal Path Cost 0  - Designated Port Id 0x838a
%   ge2: Configured Internal Path Cost 20000
%   ge2: Configured CST External Path cost 20000
%   ge2: CST Priority 128  - MSTI Priority 128
%   ge2: Designated Root 80023417ebfbe9c4
%   ge2: Designated Bridge 800264006ac779a0
%   ge2: Message Age 0
%   ge2: Hello Time 2 - Forward Delay 15
%   ge2: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0

% Instance  3:  Vlans: 3

% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 800364006ac779a0
% 1: MSTI Bridge Id 800364006ac779a0
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Designated -
State Forwarding
%   ge3: Designated Internal Path Cost 0  - Designated Port Id 0x838c
%   ge3: Configured Internal Path Cost 20000
%   ge3: Configured CST External Path cost 20000
%   ge3: CST Priority 128  - MSTI Priority 128
%   ge3: Designated Root 800364006ac779a0
%   ge3: Designated Bridge 800364006ac779a0
%   ge3: Message Age 0
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
```

Verify MSTP configurations when MSTP is enabled globally.

```
#show running-config
```

```
!
bridge 1 protocol mstp
!
```

Verify MSTP configurations when MSTP is disabled globally.

```
#show running-config
!
bridge 1 protocol mstp
no bridge 1 multiple-spanning-tree enable bridge-forward
!
```

Verify MSTP configurations when MSTP instance 2 and 3 is enabled.

```
#show running-config spanning-tree
!
spanning-tree mst configuration
bridge 1  instance 2
bridge 1  instance 2 vlan 2
bridge 1  instance 3
bridge 1  instance 3 vlan 3
!
interface xe2
bridge-group 1 instance 2
!
interface xe3
bridge-group 1 instance 3
!
```

- Verify MSTP configurations when MSTP instance 2 is disabled

```
#show running-config spanning-tree
!
spanning-tree mst configuration
bridge 1 instance 3
bridge 1 instance 3 vlan 3
!
interface ge3
bridge-group 1 instance 3
!
```

Verify MSTP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1
switchport mode access
switchport access vlan 2
bridge-group 1 instance 2
!
```

Verify MSTP configurations when spanning-tree is disabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1 spanning-tree disable
switchport mode access
switchport access vlan 2
bridge-group 1 instance 2
```

Verify MSTP details after disabling spanning-tree on interface ge2 with the `show spanning-tree mst details` command.

```
#show spanning-tree mst detail
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: CIST Root Path Cost 0 - CIST Root Port 908 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% 1: CIST Root Id 80003417ebfbe9c4
% 1: CIST Reg Root Id 80003417ebfbe9c4
% 1: CIST Bridge Id 800064006ac779a0
% 1: 10 topology change(s)  - last topology change Fri Nov 25 21:21:05 2016

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Disabled -
State Forwarding
%   ge2: Designated External Path Cost 0 -Internal Path Cost 20000
%   ge2: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge2: Designated Port Id 0x838a - CIST Priority 128  -
%   ge2: Message Age 0 - Max Age 20
%   ge2: CIST Hello Time 2 - Forward Delay 15
%   ge2: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change
timer 0
%   ge2: forward-transitions 2
%   ge2: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%   ge2: Configured Link Type point-to-point - Current point-to-point
%   ge2: No auto-edge configured - Current port Auto Edge off
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Rootport -
State Forwarding
%   ge3: Designated External Path Cost 0 -Internal Path Cost 20000
%   ge3: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge3: Designated Port Id 0x838b - CIST Priority 128  -
%   ge3: CIST Root 80003417ebfbe9c4
%   ge3: Regional Root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: CIST Hello Time 2 - Forward Delay 15
%   ge3: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change
timer 0
%   ge3: forward-transitions 3
%   ge3: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
%   ge3: Configured Link Type point-to-point - Current point-to-point
%   ge3: No auto-edge configured - Current port Auto Edge off

% Instance  2:  Vlans: 2
```

```
% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 800264006ac779a0
% 1: MSTI Bridge Id 800264006ac779a0
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Disabled -
State Discarding
%   ge2: Designated Internal Path Cost 0  - Designated Port Id 0x8389
%   ge2: Configured Internal Path Cost 20000
%   ge2: Configured CST External Path cost 20000
%   ge2: CST Priority 128  - MSTI Priority 128
%   ge2: Designated Root 800264006ac779a0
%   ge2: Designated Bridge 800264006ac779a0
%   ge2: Message Age 0
%   ge2: Hello Time 2 - Forward Delay 15
%   ge2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

% Instance  3:  Vlans: 3

% 1: MSTI Root Path Cost 20000 -MSTI Root Port 5004 - MSTI Bridge Priority
32768
% 1: MSTI Root Id 80033417ebfbe9c4
% 1: MSTI Bridge Id 800364006ac779a0
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Rootport -
State Forwarding
%   ge3: Designated Internal Path Cost 0  - Designated Port Id 0x838b
%   ge3: Configured Internal Path Cost 20000
%   ge3: Configured CST External Path cost 20000
%   ge3: CST Priority 128  - MSTI Priority 128
%   ge3: Designated Root 80033417ebfbe9c4
%   ge3: Designated Bridge 800364006ac779a0
%   ge3: Message Age 0
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1
```

STP Configuration

Bridge 1

Disabling STP globally

`Bridge1(config)#no bridge 1 spanning-tree enable bridge-forward`	Disable spanning tree globally for STP.
`Bridge1(config)#commit`	Commit the configure on the node.

Disabling STP per port

`Bridge1(config)#interface ge2`	Enter interface mode for ge2.
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for STP and put port on forwarding state. This command disables any type of STP on the port.
`Bridge1(config-if)#commit`	Commit the configure on the node.

Bridge 2

Disabling STP globally

`Bridge2(config)#no bridge 1 spanning-tree enable bridge-forward`	Disable spanning tree globally for STP.
`Bridge2(config)#commit`	Commit the configure on the node.

Disabling STP per port

`Bridge2(config)#interface xe2`	Enter interface mode for xe2.
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for STP and put port on forwarding state. This command disables any type of STP on the port.
`Bridge2(config-if)#commit`	Commit the configure on the node.

Validation

Bridge 1

Verify STP details when stp is enabled globally and ge2 and ge3 are part of the bridge using the `show spanning-tree` command.

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled - topology change
% 1: Root Path Cost 4 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Root port 905
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: 3 topology changes - last topology change Tue Nov 15 21:33:53 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec

%ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - path cost 4 -
designated cost 0
%ge2: Designated Port Id 0x838a - state Forwarding -Priority 128
%ge2: Designated root 80003417ebfbe9c4
%ge2: Designated Bridge 80003417ebfbe9c4
%ge2: Message Age 0 - Max Age 20
%ge2: Hello Time 2 - Forward Delay 15
%ge2: Forward Timer 0 - Msg Age Timer 18 - Hello Timer 1 - topo change  timer0
%ge2: forward-transitions 1
%ge2: No portfast configured – Current  portfast
%ge2: bpdu-guard default- Current bpdu-guard off
%ge2: bpdu-filter default- Current bpdu-filter off
%ge2: no root guard configured- Current root guard off
%ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - path cost 4 -
designated cost 0
%ge3: Designated Port Id 0x838b - state Blocked -Priority 128
%ge3: Designated root 80003417ebfbe9c4
%ge3: Designated Bridge 80003417ebfbe9c4
%ge3: Message Age 0 - Max Age 20
```

```
%ge3: Hello Time 2 - Forward Delay 15
%ge3: Forward Timer 0 - Msg Age Timer 19 - Hello Timer 1 - topo change timer0
%ge3: forward-transitions 0
%ge3: No portfast configured - Currentportfast off
%ge3: bpdu-guarddefault- Current bpdu-guard off
%ge3: bpdu-filter default- Current bpdu-filter off
%ge3: no root guard configured- Current root guard off
%
```

Verify STP configurations when STP is enabled globally.

```
#show running-config
!
bridge 1 protocol ieee vlan-bridge
!
```

Verify STP configurations when STP is disabled globally.

```
#show running-config
!
bridge 1 protocol ieee vlan-bridge
no bridge 1 spanning-tree enable bridge-forward
!
```

Verify STP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan all
!
```

Verify STP configurations when spanning-tree is disabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1 spanning-tree disable
switchport mode trunk
switchport trunk allowed vlan all
!
```

Verify STP details after disabling spanning-tree on interface ge2 with the `show spanning-tree` command.

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 4 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Root port 908
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: 5 topology changes - last topology change Fri Nov 25 21:15:35 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - path cost 4 -
designated cost 0
%   ge2: Designated Port Id 0x838a - state Disabled -Priority 128
```

```
%   ge2: Message Age 0 - Max Age 20
%   ge2: Hello Time 2 - Forward Delay 15
%   ge2: Forward Timer 0 - Msg Age Timer 18 - Hello Timer 0 - topo change
timer 23
%   ge2: forward-transitions 2
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - path cost 4 -
designated cost 0
%   ge3: Designated Port Id 0x838b - state Forwarding -Priority 128
%   ge3: Designated root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 19 - Hello Timer 1 - topo change
timer 23
%   ge3: forward-transitions 2
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
```

RSTP Configuration

Bridge 1

Disabling RSTP globally

`Bridge1(config)#no bridge 1 rapid-spanning-tree enable bridge-forward`	Disable spanning tree globally for RSTP.
`Bridge1(config)#commit`	Commit the configure on the node.

Disabling RSTP per port

`Bridge1(config)#interface ge2`	Enter interface mode for ge2.
`Bridge1(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for RSTP and put port on forwarding state. This command disables any type of STP on the port.
`Bridge1(config-if)#commit`	Commit the configure on the node.

Bridge 2

Disabling RSTP globally

`Bridge2(config)#no bridge 1 rapid-spanning-tree enable bridge-forward`	Disable spanning tree globally for RSTP.
`Bridge2(config)#commit`	Commit the configure on the node.

Disabling RSTP per port

`Bridge2(config)#interface xe2`	Enter interface mode for xe2.
`Bridge2(config-if)#bridge-group 1 spanning-tree disable`	Disable spanning tree per port for RSTP and put port on forwarding state. This command disables any type of STP on the port.
`Bridge2(config-if)#commit`	Commit the configure on the node.

Validation

Bridge 1

Verify RSTP details when rstp is enabled globally and ge2 and ge3 are part of the bridge using the `show spanning-tree` command.

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled- topology change detected
% 1: Root Path Cost 20000 - Root Port 905 -Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: last topology change Tue Nov 15 21:44:31 2016
% 1: 7 topology change(s)- last topology change Tue Nov 15 21:44:31 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport - State
Forwarding
% ge2: Designated Path Cost 0
% ge2: Configured Path Cost 20000- Add type Explicit ref count 1
% ge2: Designated Port Id 0x838a - Priority 128-
% ge2: Root 80003417ebfbe9c4
% ge2: Designated Bridge 80003417ebfbe9c4
% ge2: Message Age 0 - Max Age 20
% ge2: Hello Time 2 - Forward Delay 15
% ge2: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change timer
0
% ge2: forward-transitions 1
% ge2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% ge2: No portfast configured - Currentportfast off
% ge2: bpdu-guarddefault- Current bpdu-guard off
% ge2: bpdu-filter default- Current bpdu-filter off
% ge2: no root guard configured- Current root guard off
% ge2: Configured Link Type point-to-point - Current point-to-point
% ge2: No auto-edge configured - Current port Auto Edge off
% ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Alternate -
State Discarding
% ge3: Designated Path Cost 0
% ge3: Configured Path Cost 20000- Add type Explicit ref count 1
% ge3: Designated Port Id 0x838b - Priority 128-
% ge3: Root 80003417ebfbe9c4
% ge3: Designated Bridge 80003417ebfbe9c4
% ge3: Message Age 0 - Max Age 20
% ge3: Hello Time 2 - Forward Delay 15
```

```
% ge3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change timer
0
% ge3: forward-transitions 2
% ge3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% ge3: No portfast configured - Currentportfast off
% ge3: bpdu-guarddefault- Current bpdu-guard off
% ge3: bpdu-filter default- Current bpdu-filter off
% ge3: no root guard configured- Current root guard off
% ge3: Configured Link Type point-to-point - Current point-to-point
% ge3: No auto-edge configured - Current port Auto Edge off
%
```

Verify RSTP configurations when RSTP is enabled globally.

```
#show running-config
!
bridge 1 protocol rstp vlan-bridge
!
```

- Verify RSTP configurations when RSTP is disabled globally

```
#show running-config
!
bridge 1 protocol rstp vlan-bridge
no bridge 1 rapid-spanning-tree enable bridge-forward
!
```

Verify RSTP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan all
!
```

Verify RSTP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
!
interface ge2
switchport
bridge-group 1 spanning-tree disable
switchport mode trunk
switchport trunk allowed vlan all
```

Verify RSTP details after disabling spanning-tree on interface ge2 with the `show spanning-tree` command.

```
#sh spanning-tree
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 20000 - Root Port 908 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: last topology change Fri Nov 25 21:08:56 2016
% 1: 11 topology change(s)  - last topology change Fri Nov 25 21:08:56 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
```

```
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Disabled -
State Forwarding
%   ge2: Designated Path Cost 0
%   ge2: Configured Path Cost 20000  - Add type Explicit ref count 1
%   ge2: Designated Port Id 0x838a - Priority 128  -
%   ge2: Message Age 0 - Max Age 20
%   ge2: Hello Time 2 - Forward Delay 15
%   ge2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change timer
0
%   ge2: forward-transitions 2
%   ge2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%   ge2: Configured Link Type point-to-point - Current point-to-point
%   ge2: No auto-edge configured - Current port Auto Edge off
%
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Rootport -
State Forwarding
%   ge3: Designated Path Cost 0
%   ge3: Configured Path Cost 20000  - Add type Explicit ref count 1
%   ge3: Designated Port Id 0x838b - Priority 128  -
%   ge3: Root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1 - topo change timer
0
%   ge3: forward-transitions 3
%   ge3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
%   ge3: Configured Link Type point-to-point - Current point-to-point
%   ge3: No auto-edge configured - Current port Auto Edge off
```

CHAPTER 8 VLAN Configuration

This chapter contains an example for VLAN configuration on trunk port.

Configuring VLAN Tags

Topology

This shows configuring a VLAN bridge with VLAN tags on forwarding frames. Link between Bridge 2 and Bridge 3 is configured with VLAN 5 and VLAN 10. Link between Bridge 2 and Bridge 1 is configured as VLAN 5 and link between Bridge 3 and Bridge 1 is configured as VLAN 10.

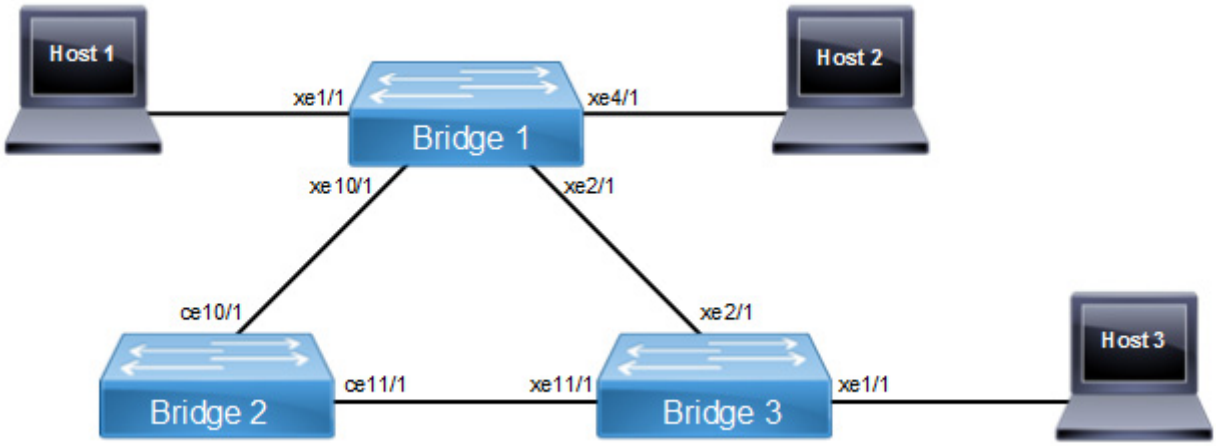


Figure 8-16: VLAN Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Bridge 1

`Bridge1#configure terminal`	Enter configuration mode
`Bridge1(config)#bridge 1 protocol ieee vlan-bridge`	Specify VLAN for bridge 1.
`Bridge1(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge1(config-vlan)#vlan 5 bridge 1 state enable`	Enable VLAN (5) on bridge 1.Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge1(config-vlan)#vlan 10 bridge 1 state enable`	Enable VLAN (10) on bridge 1. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge1(config-vlan)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge1(config)#interface xe1/1`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure port as L2.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.

`Bridge1(config-if)#switchport mode access`	Set the switching characteristics of this interface to access mode.
`Bridge1(config-if)#switchport access vlan 5`	Enable VLAN ID 5 on this port.
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge1(config)#interface xe2/1`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure port as L2.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge1(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge1(config)#interface xe4/1`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure port as L2.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#switchport mode access`	Set the switching characteristics of this interface to access mode.
`Bridge1(config-if)#switchport access vlan 10`	Enable VLAN ID 10 on this port.
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge1(config)#interface xe10/1`	Enter interface mode.
`Bridge1(config-if)#switchport`	Configure port as L2.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge1(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.
`Bridge1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge1(config-if)#exit`	Exit from the interface mode and go config mode.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol ieee vlan-bridge`	Specify VLAN for bridge 2.
`Bridge2(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge2(config-vlan)#vlan 5 bridge 2 state enable`	Enable VLAN (5) on bridge 2. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge2(config-vlan)#vlan 10 bridge 2 state enable`	Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.

`Bridge2(config-vlan)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge2(config)#interface ce10/1`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure port as L2.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group 2.
`Bridge2(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge2(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.
`Bridge2(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge2(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge2(config)#interface ce11/1`	Enter interface mode.
`Bridge2(config-if)#switchport`	Configure port as L2.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group 2.
`Bridge2(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge2(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.
`Bridge2(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge2(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge2(config-if)#exit`	Exit from the interface mode and go config mode.

Bridge 3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#bridge 3 protocol ieee vlan-bridge`	Specify VLAN for bridge 3.
`Bridge3(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge3(config-vlan)#vlan 5 bridge 3 state enable`	Enable VLAN (5) on bridge 3. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge3(config-vlan)#vlan 10 bridge 3 state enable`	Enable VLAN (10) on bridge 3. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
`Bridge3(config-vlan)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge3(config)#interface xe1/1`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure port as L2.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group 3.
`Bridge3(config-if)#switchport mode access`	Set the switching characteristics of this interface to access mode.

`Bridge3(config-if)#switchport access vlan 10`	Enable VLAN ID 10 on this port.
`Bridge3(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge3(config)#interface xe2/1`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure port as L2.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group 3.
`Bridge3(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge3(config-if)#switchport trunk allowed vlan add 10`	Enable VLAN ID 10 on this port.
`Bridge3(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-if)#exit`	Exit from the interface mode and go config mode.
`Bridge3(config)#interface xe11/1`	Enter interface mode.
`Bridge3(config-if)#switchport`	Configure port as L2.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group 3.
`Bridge3(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`Bridge3(config-if)#switchport trunk allowed vlan add 5`	Enable VLAN ID 5 on this port.
`Bridge3(config-if)#commit`	Commit the candidate configuration to the running configuration.
`Bridge3(config-if)#exit`	Exit from the interface mode and go config mode.

Validation

Bridge 1

```
Bridge1#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 1 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 909
% 1: Root Id 8000001823304db6
% 1: Bridge Id 8000001823305244
% 1: 6 topology changes - last topology change Fri Apr 19 12:32:26 2019
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   xe1/1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - path cost 4 - designated
cost 1
%   xe1/1: Designated Port Id 0x8389 - state Forwarding -Priority 128
%   xe1/1: Designated root 8000001823304db6
%   xe1/1: Designated Bridge 8000001823305244
%   xe1/1: Message Age 1 - Max Age 20
%   xe1/1: Hello Time 2 - Forward Delay 15
%   xe1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
```

```
%   xe1/1: forward-transitions 1
%   xe1/1: No portfast configured - Current  portfast off
%   xe1/1: bpdu-guard  default  - Current bpdu-guard off
%   xe1/1: bpdu-filter default  - Current bpdu-filter off
%   xe1/1: no root guard configured     - Current root guard off
%
%   xe2/1: Port Number 909 - Ifindex 5005 - Port Id 0x838d - path cost 1 - designated
cost 0
%   xe2/1: Designated Port Id 0x838d - state Forwarding -Priority 128
%   xe2/1: Designated root 8000001823304db6
%   xe2/1: Designated Bridge 8000001823304db6
%   xe2/1: Message Age 0 - Max Age 20
%   xe2/1: Hello Time 2 - Forward Delay 15
%   xe2/1: Forward Timer 0 - Msg Age Timer 19 - Hello Timer 0 - topo change timer 0
%   xe2/1: forward-transitions 2
%   xe2/1: No portfast configured - Current  portfast off
%   xe2/1: bpdu-guard  default  - Current bpdu-guard off
%   xe2/1: bpdu-filter default  - Current bpdu-filter off
%   xe2/1: no root guard configured     - Current root guard off
%
%   xe4/1: Port Number 917 - Ifindex 5013 - Port Id 0x8395 - path cost 4 - designated
cost 1
%   xe4/1: Designated Port Id 0x8395 - state Forwarding -Priority 128
%   xe4/1: Designated root 8000001823304db6
%   xe4/1: Designated Bridge 8000001823305244
%   xe4/1: Message Age 1 - Max Age 20
%   xe4/1: Hello Time 2 - Forward Delay 15
%   xe4/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   xe4/1: forward-transitions 1
%   xe4/1: No portfast configured - Current  portfast off
%   xe4/1: bpdu-guard  default  - Current bpdu-guard off
%   xe4/1: bpdu-filter default  - Current bpdu-filter off
%   xe4/1: no root guard configured     - Current root guard off
%
%   xe10/1: Port Number 941 - Ifindex 5037 - Port Id 0x83ad - path cost 2 - designated
cost 1
%   xe10/1: Designated Port Id 0x83ad - state Forwarding -Priority 128
%   xe10/1: Designated root 8000001823304db6
%   xe10/1: Designated Bridge 8000001823305244
%   xe10/1: Message Age 1 - Max Age 20
%   xe10/1: Hello Time 2 - Forward Delay 15
%   xe10/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   xe10/1: forward-transitions 2
%   xe10/1: No portfast configured - Current  portfast off
%   xe10/1: bpdu-guard  default  - Current bpdu-guard off
%   xe10/1: bpdu-filter default  - Current bpdu-filter off
%   xe10/1: no root guard configured     - Current root guard off
%
B1#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
```

```
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+------------------+-----+---------+
 1         1                   xe2/1        0018.23cb.fbbc     1     300
 1         1                   xe10/1       cc37.ab97.37d8     1     300
 1         5                   xe1/1        0000.11bc.5dec     1     300
 1         10                  xe4/1        0000.2d50.205c     1     300
Bridge1#


Bridge1#show vlan all bridge 1
Bridge  VLAN ID     Name          State   H/W Status      Member ports
                                                        (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ============================
1       1       default          ACTIVE  Success    xe10/1(u) xe2/1(u)
1       5       VLAN0005         ACTIVE  Success    xe1/1(u) xe10/1(t)
1       10      VLAN0010         ACTIVE  Success    xe4/1(u)xe2/1(t)


Bridge1#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+------------------+-----+---------+
 1         1                   xe2/1        0018.23cb.fbbc     1     300
 1         1                   xe10/1       cc37.ab97.37d8     1     300
 1         5                   xe1/1        0000.11bc.5dec     1     300
 1         10                  xe4/1        0000.2d50.205c     1     300
Bridge1#
```

Bridge 2

```
Bridge2#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+------------------+-----+---------+
 2         1                   ce10/1       0018.2326.166a     1     300
 2         1                   ce11/1       0018.23cb.fbe0     1     300
 2         1                   ce11/1       cc37.ab97.37d8     1     300
 2         5                   ce10/1       0000.11bc.5dec     1     300


Bridge2#show vlan all bridge 2
Bridge  VLAN ID     Name          State   H/W Status      Member ports
                                                        (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ============================
2       1       default          ACTIVE  Success    ce10/1(u) ce11/1(u)
2       5       VLAN0005         ACTIVE  Success    ce10/1(t) ce11/1(t)
2       10      VLAN0010         ACTIVE  Success    ce10/1(t) ce11/1(t)


Bridge2#show bridge
```

```
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 2         1                   ce10/1      0018.2326.166a    1     300
 2         1                   ce11/1      0018.23cb.fbe0    1     300
 2         1                   ce11/1      cc37.ab97.37d8    1     300
 2         5                   ce10/1      0000.11bc.5dec    1     300
```

Bridge 3

```
Bridge3# show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 3         1                   xe2/1       cc37.ab97.37d8    1     300
 3         5                   xe11/1      0000.11bc.5dec    1     300
 3         10                  xe2/1       0000.2d50.205c    1     300
Bridge3#show vlan all bridge 3
Bridge  VLAN ID     Name          State   H/W Status      Member ports
                                                          (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ============================
3       1       default          ACTIVE  Success    xe11/1(u) xe2/1(u)
3       5       VLAN0005         ACTIVE  Success    xe11/1(t)
3       10      VLAN0010         ACTIVE  Success    xe1/1(u) xe2/1(t)
```

CHAPTER 9 Disabling Native VLAN Configuration

This chapter contains sample configurations to check the functionality to drop the untagged traffic by disabling the native vlan by configuring acceptable-frame-type vlan-tagged.

Topology

Figure 9-17: Native VLAN Topology

Configuration

SW1

`SW1#configure terminal`	Enter configuration mode
`SW1(config)# bridge 1 protocol rstp vlan-bridge`	Create bridge
`SW1(config)#vlan database`	Enter VLAN configuration mode
`SW1(config-vlan)#vlan 2-10 bridge 1 state enable`	Create 2-10 vlans
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#interface xe6`	Enter interface configuration mode for xe6
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode hybrid`	Configure port mode as hybrid
`SW1(config-if)# switchport hybrid allowed vlan all`	Allow all the vlans on the xe6 port
`SW1(config-if)#exit`	Exit from interface mode
`SW1(config)#interface xe21`	Enter interface configuration mode for xe21
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode hybrid`	Configure port mode as hybrid
`SW1(config-if)# switchport hybrid allowed vlan all`	Allow all the vlans on the xe21 port
`SW1(config-if)#exit`	Exit from interface mode
`SW1(config)#commit`	Commit the candidate configuration to the running configuration

SW2

SW2#configure terminal	Enter configuration mode
SW2(config)# bridge 1 protocol rstp vlan-bridge	Create bridge
SW2(config)#vlan database	Enter VLAN configuration mode
SW2(config-vlan)#vlan 2-10 bridge 1 state enable	Create 2-10 vlans
SW2(config-vlan)#exit	Exit VLAN configuration mode
SW2(config)#interface xe6	Enter interface configuration mode for xe6
SW2(config-if)#switchport	Configure switchport
SW2(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW2(config-if)#switchport mode hybrid	Configure port mode as hybrid
SW2(config-if)# switchport hybrid allowed vlan all	Allow all the vlans on the xe6 port
SW2(config-if)#exit	Exit from interface mode
SW2(config)#interface xe13	Enter interface configuration mode for xe13
SW2(config-if)#switchport	Configure switchport
SW2(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW2(config-if)#switchport mode hybrid	Configure port mode as hybrid
SW2(config-if)# switchport hybrid allowed vlan all	Allow all the vlans on the xe13 port
SW2(config-if)#exit	Exit from interface mode
SW2(config)#commit	Commit the candidate configuration to the running configuration

Validation

Sending untagged, vlan-5 and vlan-6 traffic from ixia-1 to ixia-2. In the show bridge o/p we can see all the mac entries learnt for all the traffics.

In the show vlan brief output for default vlan interface xe21 is having port type as untagged (u).

```
SW1#show bridge
bridge 1 is running on rstp vlan-bridge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         1                   xe21        0000.0000.0003    1     300
 1         5                   xe21        0000.0000.0005    1     300
 1         6                   xe21        0000.0000.0006    1     300

SW1#sh int counters rate mbps
+------------------+-------------+------------+-------------+-------------+
|     Interface    |    Rx mbps  |    Rx pps  |    Tx mbps  |    Tx pps   |
+------------------+-------------+------------+-------------+-------------+
 ce53                0.00           0             0.00           0
```

```
 xe6                0.00           0             2960.63        246719
 xe8                0.00           0             0.00           0
 xe9                0.00           0             0.00           0
 xe21               2960.63        246719        0.00           0

SW1#sh vlan brief
Bridge  VLAN ID     Name          State   H/W Status      Member ports
                                                        (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
1       1       default          ACTIVE  Success    xe6(u) xe21(u)
1       2       VLAN0002         ACTIVE  Success    xe6(t) xe21(t)
1       3       VLAN0003         ACTIVE  Success    xe6(t) xe21(t)
1       4       VLAN0004         ACTIVE  Success    xe6(t) xe21(t)
1       5       VLAN0005         ACTIVE  Success    xe6(t) xe21(t)
1       6       VLAN0006         ACTIVE  Success    xe6(t) xe21(t)
1       7       VLAN0007         ACTIVE  Success    xe6(t) xe21(t)
1       8       VLAN0008         ACTIVE  Success    xe6(t) xe21(t)
1       9       VLAN0009         ACTIVE  Success    xe6(t) xe21(t)
1       10      VLAN0010         ACTIVE  Success    xe6(t) xe21(t)
```

Configuring acceptable-frame-type vlan-tagged on ingress interface

SW1

`SW1(config)#interface xe21`	Enter interface configuration mode for xe21
`SW1(config-if)# switchport mode hybrid acceptable-frame-type vlan-tagged`	Configure acceptable-frame-type vlan-tagged
`SW1(config-if)#exit`	Exit from interface mode
`SW1(config)#commit`	Commit the candidate configuration to the running configuration

Validation

After configuring acceptable-frame-type vlan-tagged, In the show bridge o/p we can see that un-tagged traffic is dropped (.0003 mac entry is not present), and traffic also getting dropped for that specific stream.

Now on show vlan brief output we can see that xe21 interface is having port type as tagged (t).

```
SW1#sh show bridge
bridge 1 is running on rstp vlan-bridge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+------------------+-----+---------+
 1         5                   xe21         0010.9400.0003     1     300
 1         6                   xe21         0010.9400.0004     1     300
SW1#sh int counters rate mbps
```

```
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 ce53                0.00           0             0.00           0
 xe6                 0.00           0             1971.13        164480
 xe8                 0.00           0             0.00           0
 xe9                 0.00           0             0.00           0
 xe21                2960.64        246720        0.00           0

SW1#sh vlan brief
Bridge  VLAN ID     Name         State   H/W Status      Member ports
                                                         (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ============================
1       1       default          ACTIVE  Success    xe6(u) xe21(t)
1       2       VLAN0002         ACTIVE  Success    xe6(t) xe21(t)
1       3       VLAN0003         ACTIVE  Success    xe6(t) xe21(t)
1       4       VLAN0004         ACTIVE  Success    xe6(t) xe21(t)
1       5       VLAN0005         ACTIVE  Success    xe6(t) xe21(t)
1       6       VLAN0006         ACTIVE  Success    xe6(t) xe21(t)
1       7       VLAN0007         ACTIVE  Success    xe6(t) xe21(t)
1       8       VLAN0008         ACTIVE  Success    xe6(t) xe21(t)
1       9       VLAN0009         ACTIVE  Success    xe6(t) xe21(t)
1       10      VLAN0010         ACTIVE  Success    xe6(t) xe21(t)
```

CHAPTER 10 Disabling Native VLAN Configuration on Trunk mode

This chapter contains sample configurations to check the functionality to drop the untagged traffic by disabling the native VLAN by configuring disable-native-VLAN.

Topology

Figure 10-18: Native VLAN Topology

Configuration

SW1

`SW1#configure terminal`	Enter configuration mode
`SW1(config)#bridge 1 protocol mstp`	Create bridge
`SW1(config)#vlan database`	Enter VLAN configuration mode
`SW1(config-vlan)#vlan 2-10 bridge 1 state enable`	Create 2-10 vlans
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#interface xe21`	Enter interface configuration mode for xe21
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode trunk`	Configure port mode as trunk
`SW1(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe21 port
`SW1(config-if)#exit`	Exit from interface mode
`SW1(config)#interface xe6`	Enter interface configuration mode for xe6
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode trunk`	Configure port mode as trunk
`SW1(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe6 port
`SW1(config-if)#exit`	Exit from interface mode
`SW1(config)#commit`	Commit the candidate configuration to the running configuration

SW2

`SW2#configure terminal`	Enter configuration mode
`SW2(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge
`SW2(config)#vlan database`	Enter VLAN configuration mode
`SW2(config-vlan)#vlan 2-10 bridge 1 state enable`	Create 2-10 vlans
`SW2(config-vlan)#exit`	Exit VLAN configuration mode
`SW2(config)#interface xe6`	Enter interface configuration mode for xe6
`SW2(config-if)#switchport`	Configure switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode trunk`	Configure port mode as trunk
`SW2(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe6 port
`SW2(config-if)#exit`	Exit from interface mode
`SW2(config)#interface xe13`	Enter interface configuration mode for xe13
`SW2(config-if)#switchport`	Configure switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode trunk`	Configure port mode as trunk
`SW2(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe13 port
`SW2(config-if)#exit`	Exit from interface mode
`SW2(config)#commit`	Commit the candidate configuration to the running configuration

Validation

Sending untagged, VLAN-5 and VLAN-6 traffic from IXIA-1 to IXIA-2. In the show bridge output we can see all the MAC entries learnt for all the traffics.

In the `show vlan brief` output for default VLAN interface xe21 is having port type as untagged (u).

```
SW1#show bridge
bridge 1 is running on mstp
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         1                   xe21        0010.9400.0001    1     300

SW1#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe21               621.21         606650        0.00           0
 xe6                0.00           0             621.21         606651
```

```
SW1#show vlan brief
Bridge  VLAN ID     Name          State   H/W Status      Member ports
                                                        (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
1       1       default          ACTIVE  Success    xe21(u) xe6(u)
1       2       VLAN0002         ACTIVE  Success    xe21(t) xe6(t)
1       3       VLAN0003         ACTIVE  Success    xe21(t) xe6(t)
1       4       VLAN0004         ACTIVE  Success    xe21(t) xe6(t)
1       5       VLAN0005         ACTIVE  Success    xe21(t) xe6(t)
1       6       VLAN0006         ACTIVE  Success    xe21(t) xe6(t)
1       7       VLAN0007         ACTIVE  Success    xe21(t) xe6(t)
1       8       VLAN0008         ACTIVE  Success    xe21(t) xe6(t)
1       9       VLAN0009         ACTIVE  Success    xe21(t) xe6(t)
1       10      VLAN0010         ACTIVE  Success    xe21(t) xe6(t)
```

Configuring Disable-Native-VLAN on Trunk mode

SW1

`SW1(config)#interface xe21`	Enter interface configuration mode for xe21
`SW1(config-if)#switchport mode trunk disable-native-vlan`	Configure disable native VLAN on trunk mode
`SW1(config-if)#exit`	Exit from interface mode
`SW1(config)#commit`	Commit the candidate configuration to the running configuration

Validation

After configuring disable-native-vlan, `show vlan brief` output we can see that xe21 interface is having port type as tagged (t).

```
SW1#show bridge
bridge 1 is running on mstp
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         1                   xe21       0010.9400.0001    1     300

SW1SW1#show vlan brief
Bridge  VLAN ID     Name          State   H/W Status      Member ports
                                                        (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
1       1       default          ACTIVE  Success    xe21(t) xe6(u)
1       2       VLAN0002         ACTIVE  Success    xe21(t) xe6(t)
1       3       VLAN0003         ACTIVE  Success    xe21(t) xe6(t)
1       4       VLAN0004         ACTIVE  Success    xe21(t) xe6(t)
1       5       VLAN0005         ACTIVE  Success    xe21(t) xe6(t)
```

```
1       6       VLAN0006         ACTIVE  Success    xe21(t) xe6(t)
1       7       VLAN0007         ACTIVE  Success    xe21(t) xe6(t)
1       8       VLAN0008         ACTIVE  Success    xe21(t) xe6(t)
1       9       VLAN0009         ACTIVE  Success    xe21(t) xe6(t)
1       10      VLAN0010         ACTIVE  Success    xe21(t) xe6(t)

SW1#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 Xe21                864.88          844613         0.00            0
 Xe6                0.00            0              0.00           0

SW1#show interface counters drop-stats
Interface xe21
  Rx Policy Discards: 454522965
  Rx EGR Port Unavail: 454522967
```

CHAPTER 11 802.1X Configuration

IEEE 802.1x restricts unauthenticated devices from connecting to a switch. Only after authentication is successful, traffic is allowed through the switch.

Topology

In this example, a radius server keeps the client information, validating the identity of the client and updating the switch about the authentication status of the client. The switch is the physical access between the two clients and the server. It requests information from the client, relays information to the server and then back to the client. To configure 802.1x authentication, enable authentication on ports eth1 and eth2 and specify the radius server IP address and port.

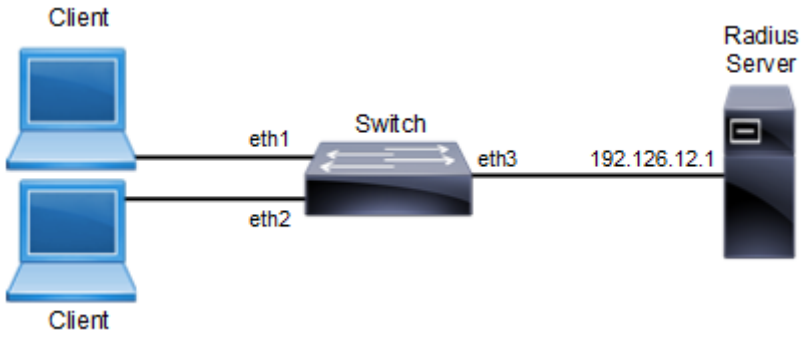


Figure 11-19: 802.1x Topology

Switch Configuration

`Switch#configure terminal`	Enter configure mode.
`Switch(config)#port-security disable`	Disable the port-security.
`Switch(config)#dot1x system-auth-ctrl`	Enable authentication globally.
`Switch(config)#interface eth2`	Enter interface mode.
`Switch(config-if)#switchport`	Enable switch port on interface.
`Switch(config-if)#dot1x port-control auto`	Enable authentication (via Radius) on port (`eth2`).
`Switch(config-if)#exit`	Exit interface mode.
`Switch(config)#interface eth1`	Enter interface mode.
`Switch(config-if)#switchport`	Enable switch port on interface.
`Switch(config-if)#dot1x port-control auto`	Enable authentication (via Radius) on port (`eth1`).
`Switch(config-if)#exit`	Exit interface mode.
`Switch(config)#radius-server dot1x key-string testing123`	Specify key with string name between radius server and client
`Switch(config)#radius-server dot1x host 192.126.12.1`	Specify the Radius Server address (192.126.12.1)
`Switch(config-radius-server)#exit`	Exit from radius server mode.
`Switch(config)#interface eth3`	Enter interface mode.
`Switch(config-if)#ip address 192.126.12.2/24`	Set the IP address on interface `eth3`.
`Switch(config-if)#commit`	Commit the transaction.
`Switch(config-if)#exit`	Exit interface mode.

Validation

show dot1x, show dot1x all

```
#show dot1x all
802.1X Port-Based Authentication Enabled
  RADIUS server address: 192.126.12.1:1812
  Next radius message id: 0
  RADIUS client address: not configured

802.1X info for interface ge1
  Supplicant address: 0000.0000.0000
  portEnabled: true - portControl: Auto
  portStatus: Unauthorized - currentId: 1
  protocol version: 2
  reAuthenticate: disabled
  reAuthPeriod: 3600
  abort:F fail:F start:F timeout:F success:F
  PAE: state: Connected - portMode: Auto
  PAE: reAuthCount: 0 - rxRespId: 0
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Invalid - reqCount: 0 - idFromServer: 0
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: in - operControlledDirections: in
  CD: bridgeDetected: false
  KR: rxKey: false
  KT: keyAvailable: false - keyTxEnabled: false


#show dot1x
802.1X Port-Based Authentication Enabled
  RADIUS server address: 192.126.12.1:1812
  Next radius message id: 0
  RADIUS client address: not configured
```

CHAPTER 12 Link Aggregation Configuration

This chapter contains a complete sample Link Aggregation Group configuration.

LACP is based on the 802.3ad IEEE specification. It allows bundling of several physical interfaces to form a single logical channel providing enhanced performance and redundancy. The aggregated interface is viewed as a single link to each switch. The spanning tree views it as one interface and not as two or three interfaces. When there is a failure in one physical interface, the other interfaces stay up and there is no disruption. Traffic can be load balanced within an LACP trunk group in a controlled manner using the hashing algorithm.

The maximum number of physical Ethernet links in a single logical channel depends upon the hardware support. Table 12-1 lists the number of LAG groups per device and number of port settings per LAG group for the QMX, QUX, and QAX hardware.

Table 12-1: Number of LAGs and ports supported

Hardware	Number of LAG groups per device	Number of port settings per LAG group
QMX	256	64
QUX	32	64
QAX	256	64

Note:

- Physical interfaces inherit the properties of LAG port once it is attached to be part of LAG, irrespective of the configuration present on the physical interface.
- In case of dynamic LAG and static LAG, member ports could be moved from one LAG to another LAG, without unconfiguring the member port.
- LAG port should be configured as a switch or router port, before adding member ports into it.

Topology

In Figure 12-20, 3 links are configured between the two switches SW1 and SW2. These three links are assigned the same administrative key (1) so that they aggregate to form a single channel 1. They are viewed by the STP as one interface.

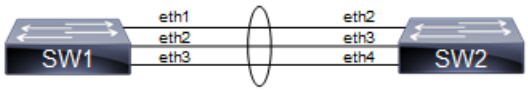


Figure 12-20: LACP topology

Dynamic LAG Configuration

SW1

`SW1#configure terminal`	Enter configure mode.
`SW1(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge

SW1(config)# vlan database	Enter VLAN database mode.
SW1(config-vlan)# vlan 2-10 bridge 1 state enable	Configure a VLAN and add it to the bridge.
SW1(config-vlan)# commit	Commit the candidate configuration to the running Configuration.
SW1(config-vlan)# exit	Exit the VLAN configuration mode.
SW1(config)#lacp system-priority 20000	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
SW1(config)#interface po10	Enter into port channel interface po10.
SW1(config-if)#switchport	Configure po10 as a layer 2 port.
SW1(config-if)#bridge-group 1	Associate bridge to an interface.
SW1(config-if)#switchport mode trunk	Configure port as a trunk.
SW1(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the po10 interface.
SW1(config-if)#commit	Commit the candidate configuration to the running Configuration.
SW1(config-if)#exit	Exit interface mode.
SW1(config)#interface eth1	Enter interface mode.
SW1(config-if)#channel-group 10 mode active	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
SW1(config-if)#commit	Commit the candidate configuration to the running Configuration.
SW1(config-if)#exit	Exit interface mode.
SW1(config)#interface eth2	Enter interface mode.
SW1(config-if)#channel-group 10 mode active	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
SW1(config-if)#commit	Commit the candidate configuration to the running Configuration.
SW1(config-if)#exit	Exit interface mode.
SW1(config)#interface eth3	Enter interface mode.
SW1(config-if)#channel-group 10 mode active	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
SW1(config-if)#commit	Commit the candidate configuration to the running Configuration.
SW1(config-if)#exit	Exit interface mode.

SW2

SW2#configure terminal	Enter configure mode.
SW2(config)# bridge 1 protocol mstp	Configure bridge 1 as MSTP bridge
SW2(config)# vlan database	Enter VLAN database mode.

`SW2(config-vlan)# vlan 2-10 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`SW2(config-vlan)# commit`	Commit the candidate configuration to the running Configuration.
`SW2(config-vlan)# exit`	Exit the VLAN configuration mode.
`SW2(config)#lacp system-priority 20000`	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
`SW2(config)#interface po10`	Enter into port channel interface po10.
`SW2(config-if)#switchport`	Configure po10 as a layer 2 port.
`SW2(config-if)#bridge-group 1`	Associate bridge to an interface.
`SW2(config-if)#switchport mode trunk`	Configure port as a trunk.
`SW2(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the po10 interface.
`SW2(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`SW2(config-if)#exit`	Exit interface mode.
`SW2(config)#interface eth2`	Enter interface mode.
`SW2(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`SW2(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`SW2(config-if)#exit`	Exit interface mode.
`SW2(config)#interface eth3`	Enter interface mode.
`SW2(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`SW2(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`SW2(config-if)#exit`	Exit interface mode.
`SW2(config)#interface eth4`	Enter interface mode.
`SW2(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`SW2(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`SW2(config-if)#exit`	Exit interface mode.

Validation

show etherchannel detail, show etherchannel summary, show running-config interface po10, show running-config interface eth1

```
#show etherchannel detail
% Aggregator po10 7
% Aggregator Type: Layer2
%  Mac address: 08:00:27:50:6a:9b
```

```
%  Admin Key: 0010 - Oper Key 0010
%  Actor LAG ID- 0x4e20,08-00-27-ab-ea-38,0x000a
%  Receive link count: 3 - Transmit link count: 3
%  Individual: 0 - Ready: 1
%  Partner LAG ID- 0x4e20,08-00-27-f8-3c-30,0x000a
%   Link: eth1 (3) sync: 1
%   Link: eth2 (4) sync: 1
%   Link: eth3 (5) sync: 1
%   Collector max delay: 5

#show etherchannel summary
% Aggregator po10 7
% Aggregator Type: Layer2
% Admin Key: 0010 - Oper Key 0010
% Aggregator Type: Layer2
%   Link: eth1 (3) sync: 1
%   Link: eth2 (4) sync: 1
%   Link: eth3 (5) sync: 1

#show running-config interface po10
!
interface po10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all

#show running-config interface eth1
!
interface eth1
 channel-group 10 mode active
```

Static LAG Configuration

SW1

`SW1#configure terminal`	Enter configure mode.
`SW1(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge
`SW1(config)# vlan database`	Enter VLAN database mode.
`SW1(config-vlan)# vlan 2-10 bridge 1 state enable`	Configure a VLAN and add it to the bridge.
`SW1(config-vlan)# commit`	Commit the candidate configuration to the running Configuration.
`SW1(config-vlan)# exit`	Exit the VLAN configuration mode.
`SW1(config)#lacp system-priority 20000`	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
`SW1(config)#interface sa10`	Enter into port channel interface sa10.
`SW1(config-if)#switchport`	Configure sa10 as a layer 2 port.
`SW1(config-if)#bridge-group 1`	Associate bridge to an interface.

SW1(config-if)#switchport mode trunk	Configure port as a trunk.
SW1(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the po10 interface.
SW1(config-if)#commit	Commit the candidate configuration to the running Configuration.
SW1(config-if)#exit	Exit interface mode.
SW1(config)#interface eth1	Enter interface mode.
SW1(config-if)#static-channel-group 10	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
SW1(config-if)#commit	Commit the candidate configuration to the running Configuration.
SW1(config-if)#exit	Exit interface mode.
SW1(config)#interface eth2	Enter interface mode.
SW1(config-if)#static-channel-group 10	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
SW1(config-if)#commit	Commit the candidate configuration to the running Configuration.
SW1(config-if)#exit	Exit interface mode.
SW1(config)#interface eth3	Enter interface mode.
SW1(config-if)#static-channel-group 10	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
SW1(config-if)#commit	Commit the candidate configuration to the running Configuration.
SW1(config-if)#exit	Exit interface mode.

SW2

SW2#configure terminal	Enter configure mode.
SW2(config)# bridge 1 protocol mstp	Configure bridge 1 as MSTP bridge
SW2(config)# vlan database	Enter VLAN database mode.
SW2(config-vlan)# vlan 2-10 bridge 1 state enable	Configure a VLAN and add it to the bridge.
SW2(config-vlan)# commit	Commit the candidate configuration to the running Configuration.
SW2(config-vlan)# exit	Exit the VLAN configuration mode.
SW2(config)#interface sa10	Enter into port channel interface sa10.
SW2(config-if)#switchport	Configure sa10 as a layer 2 port.
SW2(config-if)#bridge-group 1	Associate bridge to an interface.
SW2(config-if)#switchport mode trunk	Configure port as a trunk.
SW2(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the po10 interface.
SW2(config-if)#commit	Commit the candidate configuration to the running Configuration.
SW2(config-if)#exit	Exit interface mode.

SW2(config)#interface eth2	Enter interface mode.
SW2(config-if)#static-channel-group 10	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
SW2(config-if)#commit	Commit the candidate configuration to the running Configuration.
SW2(config-if)#exit	Exit interface mode.
SW2(config)#interface eth3	Enter interface mode.
SW2(config-if)#static-channel-group 10	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
SW2(config-if)#exit	Exit interface mode.
SW2(config)#interface eth4	Enter interface mode.
SW2(config-if)#static-channel-group 10	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
SW2(config-if)#commit	Commit the candidate configuration to the running Configuration.
SW2(config-if)#exit	Exit interface mode.

Validation

```
#show static-channel-group
% Static Aggregator: sa10
% Member status:
   eth1    up
   eth2    up
   eth3    up

#show running-config interface sa10
!
interface sa10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all

#show running-config interface eth1
!
interface eth1
 static-channel-group 10
```

Static LAG Minimum Link Configuration

Configure the minimum number of ports that must be linked up and bundled in the LACP port channel. We can configure the minimum links range from 2 to 32. If the number of ports aggregated to the port channel is less than the minimum number of links configured, then the port channel enters the Protocol Down because of the minimum link state.

Note: Minimum links must be configured only on one side of static channel for optimal performance.

Topology

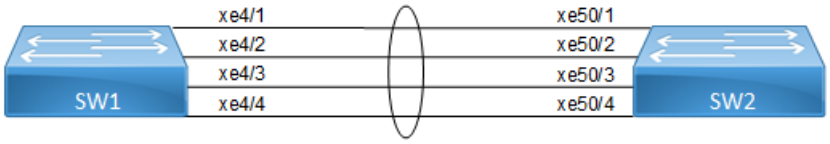


Figure 12-21: LAG minimum link

SW1

`#configure terminal`	Enter configure mode.
`(config)#interface sa10`	Creating interface static-lag sa10
`(config-if)#port-channel min-links 4`	Configuring port channel minimum links as 4(range is 2-32)
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode

SW2

`#configure terminal`	Enter configure mode.
`(config)#interface sa10`	Creating interface port-channel sa10
`(config-if)#port-channel min-links 4`	Configuring port channel minimum links as 4 (range is 2-32)
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode

Validation

SW1

```
#show static-channel-group 10
% Static Aggregator: sa10
% Minimum-Links 4
% Member status:
         xe4/1      up
         xe4/2      up
         xe4/3      up
         xe4/4      up



#show running-config interface sa10
!
interface sa10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel min-links 4
```

SW2

```
#show running-config interface sa10
!
interface sa10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel min-links 4
!

#show static-channel-group 10
% Static Aggregator: sa10
% Minimum-Links 4
% Member status:
         Xe50/1     up
         Xe50/2     up
         Xe50/3     up
         Xe50/4     up
```

Note: When a sa goes down due to the minimum links configured (number of minimum links is greater than the links aggregated to the sa).

```
SW1:
=====
#sh int brief sa10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------
--
sa10         AGG   1     trunk             down     PD(Min L/B)  0
#

SW2:
=====

#sh int brief sa10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
```

```
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
--
sa10          AGG   1     trunk             down     PD(Min L/B)  0
#
```

Static-LAG Minimum Bandwidth Configuration

Configure the minimum bandwidth allowed for ports that must be linked up and bundled in the LACP port channel. We can configure the minimum bandwidth range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits. If the Total bandwidth of ports aggregated to the port channel is less than the minimum Bandwidth value configured, then the port channel enters the Protocol Down because of the minimum Bandwidth state.

Note: Minimum Bandwidth should be configured the same on both sides for optimal performance.

Topology

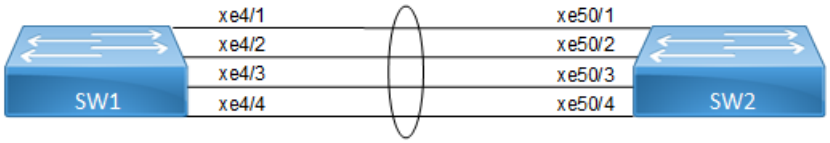


Figure 12-22: LAG minimum bandwidth

SW1

`#configure terminal`	Enter configure mode.
`(config)#interface sa10`	Creating interface static-lag sa10
`(config-if)#port-channel min-bandwidth 40g`	Configuring port channel minimum bandwidth as 40g (range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.)
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode

SW2

`#configure terminal`	Enter configure mode.
`(config)#interface sa10`	Creating interface port-channel sa10
`(config-if)#port-channel min-bandwidth 40g`	Configuring port channel minimum bandwidth as 40g (range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.)
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode

Validation

SW1

```
#show static-channel-group 10
% Static Aggregator: sa10
% Minimum- 4
% Member status:
         xe4/1     up
         xe4/2     up
         xe4/3     up
         xe4/4     up



#show running-config interface sa10
!
interface sa10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel min-links 40g
```

SW2

```
#show running-config interface sa10
!
interface sa10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel min-bandwidth 40g
!

#show static-channel-group 10
% Static Aggregator: sa10
% Minimum-bandwidth 40g
% Member status:
         Xe50/1     up
         Xe50/2     up
```

```
          Xe50/3     up
          Xe50/4     up
```

Note: When sa goes down due to [Total Bandwidth of sa] <[Minimum Bandwidth value Configured]

```
SW1:
=====
#sh int brief sa10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD - ESI Hold Timer Down


--------------------------------------------------------------------------------
--
Port-channel Type PVID Mode              Status   Reason Speed
Interface
--------------------------------------------------------------------------------
--
sa10         AGG   1     trunk             down     PD(Min L/B)  0
#


SW2:
=====

#sh int brief sa10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
```

```
-------------------------------------------------------------------------
--
sa10          AGG    1      trunk              down      PD(Min L/B)   0
#
```

Dynamic-LAG Minimum Link Configuration

Configure the minimum number of ports that must be linked up and bundled in the LACP port channel. We can configure the minimum links range from 2 to 32. If the number of ports aggregated to the port channel is less than the minimum number of links configured, then the port channel enters the Protocol Down because of the minimum link state.

Note: Minimum links should be configured the same on both sides for optimal performance.

Topology

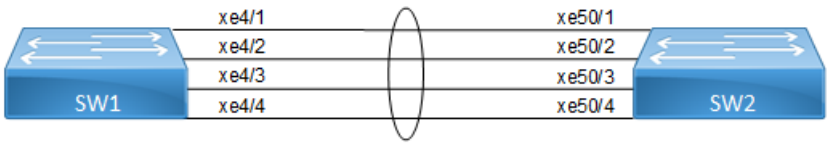


Figure 12-23: LAG minimum link

SW1

`#configure terminal`	Enter configure mode.
`(config)#interface po10`	Creating interface port-channel po10
`(config-if)#port-channel min-links 4`	Configuring port channel minimum links as 4 (range is 2-32)
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode

SW2

`#configure terminal`	Enter configure mode.
`(config)#interface po10`	Creating interface port-channel po10
`(config-if)#port-channel min-links 4`	Configuring port channel minimum links as 4 (range is 2-32)
`(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`(config-if)#exit`	Exit the configure mode

Validation

SW1

```
#sh running-config interface po10
```

```
interface po10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
port-channel min-links 4
!

!

#show etherchannel
-------------------------------------
% Lacp Aggregator: po10
% Min-links : 4
% Member:
   xe4/1
   xe4/2
   xe4/3
   xe4/4
-------------------------------------

#show etherchannel summary

% Aggregator po10 100010
% Aggregator Type: Layer2
% Admin Key: 0010 - Oper Key 0010
%   Link: xe4/4 (10072) sync: 1
%   Link: xe4/1 (10069) sync: 1
%   Link: xe4/2 (10070) sync: 1
%   Link: xe4/3 (10071) sync: 1
--------------------------------------
```

SW2

```
#show running-config interface po10
!
interface po10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel min-links 4
!

#show etherchannel

% Aggregator Type: Layer2
% Lacp Aggregator: po10
% Min-links: 4
% Member:
   xe50/1
   xe50/2
   xe50/3
   xe50/4

#show etherchannel summary
```

```
% Aggregator po10 100010
% Aggregator Type: Layer2
% Admin Key: 0010 - Oper Key 0010
%   Link: xe50/4 (10072) sync: 1
%   Link: xe50/1 (10069) sync: 1
%   Link: xe50/2 (10070) sync: 1
%   Link: xe50/3 (10071) sync: 1
```

Note: When a PO goes down due to the minimum links configured (number of minimum links is greater than the links aggregated to the PO).

```
SW1:
#sh int brief po10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
--
po10         AGG   1     trunk             down     PD(Min L/B)  0
#


#sh etherchannel
% Lacp Aggregator: po10
% Min-links: 4
% Protocol Down (Min L/B): True
% Member:
   xe4/1
   xe4/2
   xe4/3
   xe4/4

SW2:
#sh etherchannel
% Lacp Aggregator: po10
% Min-links: 4
% Protocol Down (Min L/B): True
% Member:
```

```
    Xe50/1
    Xe50/2
    Xe50/3
        xe50/4

#sh int brief po100

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
--
po10         AGG   1     trunk             down     PD(Min L/B)  0
#
```

Dynamic LAG Minimum Bandwidth Configuration

Configure the minimum bandwidth allowed for ports that must be linked up and bundled in the LACP port channel. We can configure the minimum bandwidth range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits. If the Total bandwidth of ports aggregated to the port channel is less than the minimum Bandwidth value configured, then the port channel enters the Protocol Down because of the minimum Bandwidth state.

Note: Minimum Bandwidth should be configured the same on both sides for optimal performance.

Topology

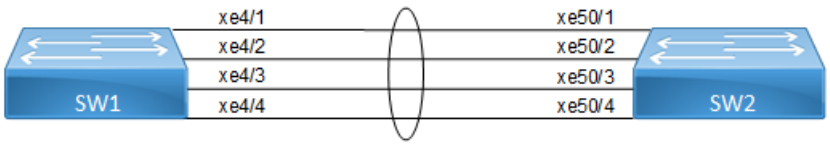


Figure 12-24: LAG minimum bandwidth

SW1

`#configure terminal`	Enter configure mode.
`(config)#interface po10`	Creating interface port-channel po10

(config-if)#port-channel min-bandwidth 40g	Configuring port channel minimum bandwidth as 40g (range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.)
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode

SW2

#configure terminal	Enter configure mode.
(config)#interface po10	Creating interface port-channel po10
(config-if)#port-channel min-bandwidth 40g	Configuring port channel minimum bandwidth as 40g (range from BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.)
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode

Validation

SW1

```
#sh running-config interface po10

interface po10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
port-channel min-bandwidth 40g
!

!

#show etherchannel
-------------------------------------
% Lacp Aggregator: po10
% Min-Bandwidth : 40g
% Member:
   xe4/1
   xe4/2
   xe4/3
   xe4/4
-------------------------------------

#show etherchannel summary

% Aggregator po10 100010
% Aggregator Type: Layer3
% Admin Key: 0010 - Oper Key 0010
%   Link: xe4/4 (10072) sync: 1
%   Link: xe4/1 (10069) sync: 1
%   Link: xe4/2 (10070) sync: 1
```

```
%   Link: xe4/3 (10071) sync: 1
-------------------------------------
```

SW2

```
#show running-config interface po10
!
interface po10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 port-channel min-bandwidth 40g
!

#show etherchannel

% Lacp Aggregator: po10
% Min-Bandwidth : 40g
% Member:
   xe50/1
   xe50/2
   xe50/3
   xe50/4

#show etherchannel summary

% Aggregator po10 100010
% Aggregator Type: Layer2
% Admin Key: 0010 - Oper Key 0010
%   Link: xe50/4 (10072) sync: 1
%   Link: xe50/1 (10069) sync: 1
%   Link: xe50/2 (10070) sync: 1
%   Link: xe50/3 (10071) sync: 1
```

Note: When a PO goes down due to the [Total bandwidth] < [minimum bandwidth configured]

```
SW1:
=====
#sh int brief po10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down
```

```
--------------------------------------------------------------------------------
--
Port-channel Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
--
po10         AGG   1     trunk             down     PD(Min L/B)  0
#


#sh etherchannel
% Lacp Aggregator: po10
% Min-Bandwidth : 40g
% Protocol Down (Min L/B): True
% Member:
   xe4/1
   xe4/2
   xe4/3
   xe4/4


SW2:
=====
#sh etherchannel
% Lacp Aggregator: po10
% Min-Bandwidth : 40g
% Protocol Down (Min L/B): True
% Member:
   Xe50/1
   Xe50/2
   Xe50/3
       xe50/4

#sh int brief po10

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
--
po10         AGG   1     trunk             down     PD(Min L/B)  0
#
```

LACP Minimum-Link, Minimum-Bandwidth on Dynamic and Static Channel-Groups with MLAG

Overview

OcNOS allows the configuration of minimum number of the LAG members per LAG group. Both these configurations are meaningful in case the LAG is used for incremental-BW mode. The minimum configuration controls the minimum number of members /bandwidth that must be operationally up / bandwidth available to declare their LAG as operationally UP.

When static/dynamic LAG interface configured with minimum links / minimum bandwidth, the following conditions are to be met:

- Ports which are admin and operational up are considered for min-link.
- The specified minimum number of links should be up.
- Min-link and min-bandwidth cannot co-exist.
- When ports are down due to min-link/min-bandwidth, in show interface brief command output, port down with the corresponding reason code for the failure due to min-link/min-bandwidth.

Minimum Active Members/Bandwidth

The user can specify the minimum number of members that must be operationally up to declare their LAG as operationally UP. Note that this parameter applies to static/dynamic LAG.

```
port-channel min-links <2 - 32>
```

The minimum active member configuration will be allowed to be modified to be greater than the current number of active members. In such configuration, the LAG operational status will become operationally down.

The user can specify the minimum bandwidth, based on the configured value and the ports that satisfy the conditions LAG will be operationally UP. This parameter is applied for static/dynamic LAG.

```
port-channel min-bandwidth BANDWIDTH
```

BANDWIDTH <1-999>k|m for 1 to 999 kilo bits or mega bits <1-1000>g for 1 to 1000 giga bits.

When condition fails, the operational state changes to DOWN.

Note: Do not configure minimum-link, Minimum Bandwidth both on TORs and Switches at the same time to avoid flaps of MLAG.

Topology

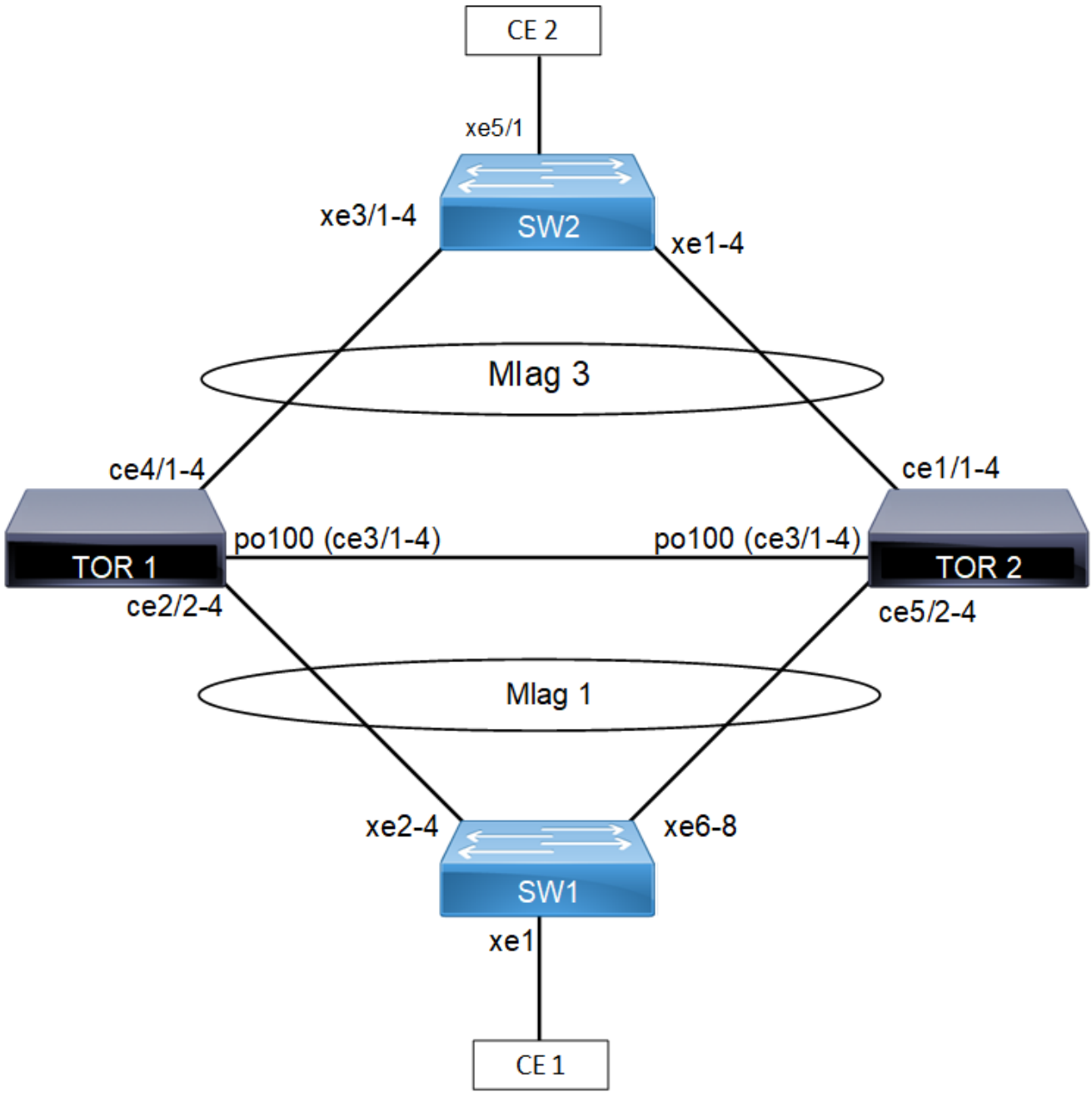


Figure 12-25: MLAG topology

Configuration

TOR1

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol rstp vlan-bridge`	Configure bridge type

(config)# vlan database	Enter vlan database
(config-vlan)# vlan 600,601,502 bridge 1 state enable	Configure vlans
(config-vlan)#commit	Commit the candidate configuration to the running Configuration.
(config-vlan)#exit	Exit the configure mode.
(config)#interface mlag1	Enter Interface mode
(config-if)# switchport	Make mlag as layer2 port
(config-if)# bridge-group 1	Attach interface to bridge
(config-if)# switchport mode trunk	Configure trunk port
(config-if)# switchport trunk allowed vlan add 600,601,502	Add interface to vlans
(config-if)# spanning-tree edgeport	Configure port as edge port to avoid loops
(config-if)# spanning-tree bpdu-filter enable	Enable bpdu filter to avoid loops
(config-if)# mtu 9216	Configure mtu.
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface mlag3	Enter Interface mode
(config-if)# switchport	Make mlag as layer2 port
(config-if)# bridge-group 1	Attach interface to bridge
(config-if)# switchport mode trunk	Configure trunk port
(config-if)# switchport trunk allowed vlan add 600,502	Add interface to vlans
(config-if)# spanning-tree edgeport	Configure port as edge port to avoid loops
(config-if)# spanning-tree bpdu-filter enable	Enable bpdu filter to avoid loops
(config-if)# mtu 9216	Configure mtu.
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface po100	Enter Interface mode
(config-if)# switchport	Make po as layer2 port
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface sa1	Enter Interface mode
(config-if)# switchport	Make sa1 as layer2 port
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)# interface sa3	Enter interface mode.
(config-if)# switchport	Make sa3 as layer2 port.
(config-if)#commit	Commit the candidate configuration to the running Configuration.

(config-if)#exit	Exit the configure mode.
(config)#interface ce2/1	Enter Interface mode
(config-if)#port breakout enable	Port breakout enabled
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce2/2	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce2/3	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce2/4	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce3/1	Enter Interface mode
(config-if)#port breakout enable	Port breakout enabled
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce3/2	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce3/3	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce3/4	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce4/1	Enter Interface mode
(config-if)#port breakout enable	Port breakout enabled

(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce4/2	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce4/3	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#mcec domain configuration	Enter Multichasis Etherchannel domain configuration mode.
(config-mcec-domain)# domain-address 1111.2222.3333	Configure the domain address.
(config-mcec-domain)# domain-system-number 1	Configure the domain system number
(config-mcec-domain)# intra-domain-link po100	Specify the intra domain link for MLAG communication
(config-mcec-domain)#commit	Commit the candidate configuration to the running Configuration.
(config-mcec-domain)#exit	Exit the configure mode.
(config)#interface sa1	Enter Interface mode
(config-if)#mlag 1	Map sa1 to mlag1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#int mlag1	Enter Interface mode
(config-if)#mode active-standby	Configure mlag mode for mlag1
(config-if)#switchover type revertive 10	Configure revertive timer
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface sa3	Enter Interface mode
(config-if)#mlag 3	Map sa3 to mlag3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#int mlag3	Enter Interface mode
(config-if)#mode active-standby	Configure mlag mode for mlag3
(config-if)#switchover type revertive 10	Configure revertive timer
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.

(config-if)# interface sa1	Enter sa interface mode
(config-if)#port-channel min-links 3	Configure min-link value on sa interface
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface sa3	Enter sa Interface mode
(config-if)#port-channel min-bandwidth 30g	Configure min-bandwidth value on sa/po interface
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.

TOR2

#configure terminal	Enter configure mode.
(config)# bridge 1 protocol rstp vlan-bridge	Configure bridge type
(config)# vlan database	Enter vlan database
(config-vlan)# vlan 600,601,502 bridge 1 state enable	Configure vlans
(config-vlan)#commit	Commit the candidate configuration to the running Configuration.
(config-vlan)#exit	Exit the configure mode.
(config)#interface mlag1	Enter Interface mode
(config-if)# switchport	Make mlag as layer2 port
(config-if)# bridge-group 1	Attach interface to bridge
(config-if)# switchport mode trunk	Configure trunk port
(config-if)# switchport trunk allowed vlan add 600,601,502	Add interface to vlans
(config-if)# spanning-tree edgeport	Configure port as edge port to avoid loops
(config-if)# spanning-tree bpdu-filter enable	Enable bpdu filter to avoid loops
(config-if)# mtu 9216	Configure mtu.
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface mlag3	Enter Interface mode
(config-if)# switchport	Make mlag as layer2 port
(config-if)# bridge-group 1	Attach interface to bridge
(config-if)# switchport mode trunk	Configure trunk port
(config-if)# switchport trunk allowed vlan add 600,502	Add interface to vlans
(config-if)# spanning-tree edgeport	Configure port as edge port to avoid loops
(config-if)# spanning-tree bpdu-filter enable	Enable bpdu filter to avoid loops
(config-if)# mtu 9216	Configure mtu.
(config-if)#commit	Commit the candidate configuration to the running Configuration.

(config-if)#exit	Exit the configure mode.
(config)#interface po100	Enter Interface mode
(config-if)# switchport	Make po(IDL) as layer2 port
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface sa1	Enter Interface mode
(config-if)# switchport	Make sa1 as layer2 port
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface sa3	Enter Interface mode
(config-if)# switchport	Make sa3 as layer2 port
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce1/1	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce1/2	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce1/3	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce3/1	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce3/2	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce3/3	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100

(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce3/4	Enter Interface mode
(config-if)# channel-group 100 mode active	Add interface to po100
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce5/1	Enter Interface mode
(config-if)# port breakout enable	Port breakout enabled
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce5/2	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce5/3	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ce5/4	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config-mcec-domain)# intra-domain-link po100	Specify the intra domain link for MLAG communication
(config-mcec-domain)#commit	Commit the candidate configuration to the running Configuration.
(config-mcec-domain)#exit	Exit the configure mode.
(config)#interface sa1	Enter Interface mode
(config-if)#mlag 1	Map sa1 to mlag1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#int mlag1	Enter Interface mode
(config-if)#mode active-standby	Configure mlag mode for mlag1
(config-if)#switchover type revertive 10	Configure revertive timer
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface sa3	Enter Interface mode

(config-if)#mlag 3	Map sa3 to mlag3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#int mlag3	Enter Interface mode
(config-if)#mode active-standby	Configure mlag mode for mlag3
(config-if)#switchover type revertive 10	Configure revertive timer
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config-if)# interface sa1	Enter sa interface mode
(config-if)#port-channel min-links 3	Configure min-link value on sa interface
(config)#interface sa3	Enter sa Interface mode
(config-if)#port-channel min-bandwidth 30g	Configure min-bandwidth value on sa interface.
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.

SW1

configure terminal	Enter Configure mode.
(config)#bridge 1 protocol rstp vlan-bridge	Configure bridge type
(config)#vlan database	Create vlan database
(config-vlan)#vlan 600,601,502,101,100,300,401,402 bridge 1 state enable	Create Vlans
(config-vlan)#commit	Commit the candidate configuration to the running Configuration.
(config-vlan)#exit	Exit the configure mode.
(config)#interface xe1	Enter Interface mode
(config-if)# switchport	Make xe1 as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#spanning-tree edgeport	Configure port as edgeport
(config-if)#spanning-tree bpdu-filter enable	Enable spanning tree bpdu filter
(config-if)# mtu 9216	Configure mtu
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface sa1	Enter Interface mode
(config-if)# switchport	Make xe1 as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.

(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed vlan add 100,101,300,401,402,502	Enable all VLAN identifiers on this interface.
(config-if)#spanning-tree edgeport	Configure port as edgeport
(config-if)#spanning-tree bpdu-filter enable	Enable spanning tree bpdu filter
(config-if)# mtu 9216	Configure mtu
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe2	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe3	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe4	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe6	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe7	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe8	Enter Interface mode
(config-if)# static-channel-group 1	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.

SW2

configure terminal	Enter Configure mode.
(config)#bridge 1 protocol rstp vlan-bridge	Configure bridge type

(config)#vlan database	Create vlan database
(config-vlan)#vlan 600,601,502,101,100,401,402 bridge 1 state enable	Create vlans
(config-vlan)#commit	Commit the candidate configuration to the running Configuration.
(config-vlan)#exit	Exit the configure mode.
(config)#interface xe5/1	Enter Interface mode
(config-if)# switchport	Make xe1 as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#spanning-tree edgeport	Configure port as edge port
(config-if)#spanning-tree bpdu-filter enable	Enable spanning tree bpdu filter
(config-if)# mtu 9216	Configure mtu
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface sa3	Enter Interface mode
(config-if)# switchport	Make sa3 as layer2 port
(config-if)# bridge-group 1	Associate the interface with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed vlan add 100,101,401,402,600,502	Enable all VLAN identifiers on this interface.
(config-if)#spanning-tree edgeport	Configure port as edge port
(config-if)#spanning-tree bpdu-filter enable	Enable spanning tree bpdu filter
(config-if)# mtu 9216	Configure mtu
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe3/1	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
#configure terminal	Enter Configure mode.
(config)#interface xe3/2	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe3/3	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3

(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe1/1	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe1/2	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe1/3	Enter Interface mode
(config-if)# static-channel-group 3	Add interface to sa3
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.

This configuration is applicable for the dynamic LAG with MLAG topology except dynamic LAG interface creations, which needs to be referred from the dynamic LAG configurations given above.

Validation

When sa or po goes down due to min-link or min-bandwidth not satisfied, below validations to be done:

TOR 1

```
#sh int brief sa1
Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down

--------------------------------------------------------------------------------
Port-channel Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
--
sa1           AGG   1     trunk             down     PD(Min L/B)  0

#
#sh int brief po100
```

```
Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down,
 IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
--
Port-channel  Type  PVID  Mode              Status   Reason  Speed
Interface
--------------------------------------------------------------------------------
--
po100         AGG   1     trunk             down     PD(Min L/B)  0

#
#sh etherchannel
% Lacp Aggregator: po100
% Min-Bandwidth : 40g
% Protocol Down (Min L/B) : True
% Member:
   ce3/1
   ce3/2
   ce3/3
   ce3/4
-----------------------------------
% Lacp Aggregator: sa1
% Min-links : 3
% Protocol Down (Min L/B): True
% Member:
   ce2/2
   ce2/3
   ce2/4
-----------------------------------
% Lacp Aggregator: sa3
% Member:
   ce4/1
   ce4/2
   ce4/3
#
#sh running-config interface sa1
!
interface sa1
 switchport
 port-channel load-balance src-dst-mac
 port-channel min-links 3
 mlag 1
!
```

```
#sh static-channel-group 1
 Static Aggregator: sa1
 Minimum-Links 3
 Member Status
  ce2/2          down
  ce2/3          down
  ce2/4          down
#
#sh etherchannel summary
  Aggregator po100 100100
  Aggregator Type: Layer2
  Admin Key: 0100 - Oper Key 0100
     Link: ce3/1 (5057) sync: 0
     Link: ce3/2 (5058) sync: 0
     Link: ce3/3 (5059) sync: 0
     Link: ce3/4 (5060) sync: 0
-------------------------------------
```

LACP Force-Up

In an aggregated environment, there are some parameters that are set for member ports in lag. Whenever the parameters are set and conditions are satisfied, the port channel will be in SYNC. If force-up mode is enabled for the member port, the port channel will always be in SYNC even if the parameters are not set i.e. the traffic will not be affected and the port channel will never go down.

LACP Force-up with Dynamic LAG

Topology

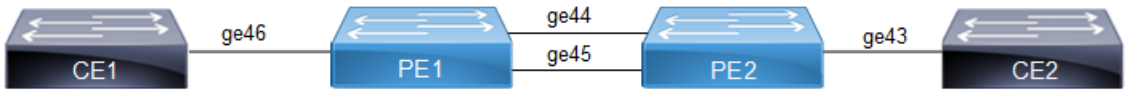


Figure 12-26: LACP force-up with dynamic LAG

CE1

`#configure terminal`	Enter configure mode.
`(config)#hostname CE1`	Configure host name
`(config)#bridge 1 protocol rstp vlan-bridge`	Create a RSTP VLAN bridge on customer side
`(config)#vlan database`	Enter VLAN database mode.
`(config-vlan)#vlan 2-100 bridge 1 state enable`	Configure VLAN for the bridge
`(config-vlan)#commit`	Commit the candidate configuration to the running Configuration.
`(config-vlan)#exit`	Exit the VLAN configure mode.
`(config)#interface ge46`	Enter interface mode
`(config-if)#switchport`	Make interface as Switchport
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode hybrid`	Configure the mode as hybrid

(config-if)#switchport hybrid allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface po1	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode hybrid	Configure the mode as hybrid
(config-if)#switchport hybrid allowed vlan all	Configure allowed vlan all for the hybrid mode
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ge44	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1
(config-if)#exit	Exit interface mode.
(config)#interface ge45	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.

CE2

#configure terminal	Enter configure mode.
(config)#hostname CE2	Configure host name
(config)#bridge 1 protocol provider-rstp edge	Create provider rstp edge bridge
(config)#vlan database	Enter vlan database mode
(config-vlan)#vlan 2-100 type customer bridge 1 state enable	Configure customer VLAN for the bridge
(config-vlan)#vlan 100 type service point-point bridge 1 state enable	Configure service VLAN for the bridge
(config)#exit	Exit vlan database mode
(config)#cvlan registration table map1 bridge 1	Creating registration table
(config-cvlan-registration)#cvlan 2-100 svlan 100	Mapping cvlan to svlan
(config-cvlan-registration)#commit	Commit the candidate configuration to the running Configuration.
(config-cvlan-registration)#exit	Exit the cvlan registration mode.
(config)#interface ge43	Enter interface mode
(config-if)#switchport	Make interface as Switchport
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode provider-network	Configure the mode as provider-network

(config-if)# switchport provider-network allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface po1	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#bridge-group 1	Associate the interface with bridge group 1
(config-if)#switchport mode customer-edge hybrid	Set the switching characteristics of this interface to customer-edge hybrid
(config-if)#switchport customer-edge hybrid allowed vlan all	Set the switching characteristics of this interface to customer-edge hybrid and allow vlan all
(config-if)#switchport customer-edge vlan registration map1	Configuring the registration table mapping on lag interface
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ge44	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1
(config-if)#lacp force-up	Enable lacp force-up for the member port interface
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface ge45	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1
(config-if)#commit	Commit the candidate configuration to the running Configuration.
(config-if)#exit	Exit the configure mode.

Send L2 traffic with incremental source mac of 1000 and with VLAN 100 from CE1 and with incremental source mac of 1000 and with SVLAN 100(TPID 0x88a8), CVLAN 100 from CE2.

Validation

CE1

```
CE1#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 2001
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 2001

CE1#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 0001 - Oper Key 0001
     Link: ge44 (5043) sync: 1
```

```
     Link: ge45 (5046) sync: 1

CE1#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 ge44                363.65         710252        772.76         1420506
 ge45                363.63         710222        0.00           0
 ge46                772.77         1420525       727.31         1420526
 po1                 728.56         1422971       774.09         1422966

CE2#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 2001
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 2001

CE2#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 ge43                774.26         1423267       784.17         1361411
 ge44                774.26         1423268       364.36         711634
 ge45                0.00           0             364.36         711634
 po1                 774.26         1423267       728.71         1423267

CE2#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 0001 - Oper Key 0001
     Link: ge44 (5020) sync: 1
     Link: ge45 (5022) sync: 1
```

On server side (PE1) to make LAG down you can unconfigure the channel-group 1 configurations and verify force-up is getting enabled in PE2.

To simulate the force-up:

`PE1(config)#interface ge44`	Enter interface mode.
`PE1(config-if)#no channel-group`	Removing channel-group configurations from interface.
`PE1(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`PE1(config)#interface ge45`	Enter interface mode.
`PE1(config-if)#no channel-group`	Removing channel-group configurations from interface.
`PE1(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`PE1(config-if)#exit`	Exit interface mode.

PE2

```
PE2#show interface brief | include po1
po1           AGG   1     customer-edge     up       none    1g

PE2#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 0001 - Oper Key 0001
     Link: ge44 (5020) sync: 0 (force-up)
     Link: ge45 (5022) sync: 0

PE2#show etherchannel detail
 Aggregator po1 100001
 Aggregator Type: Layer2
  Mac address: b8:6a:97:4d:65:d5
  Admin Key: 0001 - Oper Key 0001
   Actor LAG ID- 0x8000,b8-6a-97-28-a5-c0,0x0001
   Receive link count: 0 - Transmit link count: 0
   Individual: 0 - Ready: 1
  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
    Link: ge44 (5020) sync: 0 (force-up)
    Link: ge45 (5022) sync: 0
  Collector max delay: 5
```

To forward traffic from ge44 of PE1:

`PE1(config)#interface ge44`	Enter interface mode.
`PE1(config-if)#switchport`	Make the interface as switch port.
`PE1(config-if)#bridge-group 1`	Associate the interface to bridge.
`PE1(config-if)#switchport mode hybrid`	Configure the mode as hybrid.
`PE1(config-if)#switchport hybrid allowed vlan all`	Configure allowed vlan all for the hybrid mode.
`PE1(config-if)#commit`	Commit the candidate configuration to the running Configuration.
`PE1(config-if)#exit`	Exit the configure mode.

```
PE2#show interface counters rate mbps
+------------------+-------------+------------+-------------+------------+
|     Interface    |    Rx mbps  |    Rx pps  |    Tx mbps  |    Tx pps  |
+------------------+-------------+------------+-------------+------------+
 ge43               774.25        1423257      784.17        1361400
 ge44               774.25        1423258      728.71        1423257
 ge45               0.00          0            0.00          0
 po1                774.25        1423247      728.70        1423245
 PE2#
PE1#show interface counters rate mbps
+------------------+-------------+------------+-------------+------------+
|     Interface    |    Rx mbps  |    Rx pps  |    Tx mbps  |    Tx pps  |
```

```
+--------------------+--------------+-------------+--------------+-------------+
 ge44                657.67         1284505       640.77         1177884
 ge45                0.00           0             0.00           0
 ge46                772.71         1420426       603.08         1177886
```

Port-Channel Weight

Use the `port-channel weight` command to configure weighted load balancing on port-channel member links. As per the weights configured, traffic distribution will be happening across the member interfaces.

Consider if ports xe1 and xe2 associated with the L2 lag, having default load-balance as src-dst-mac and by default, best traffic distribution can happen up to 50% on each link (by varying source and destination MACs). After weight configured as 2 on interface xe1, the best traffic distribution can happen as 66.66% and 33.33% on xe1 and xe2 respectively.

Port-Channel Weight with Dynamic LAG

Topology

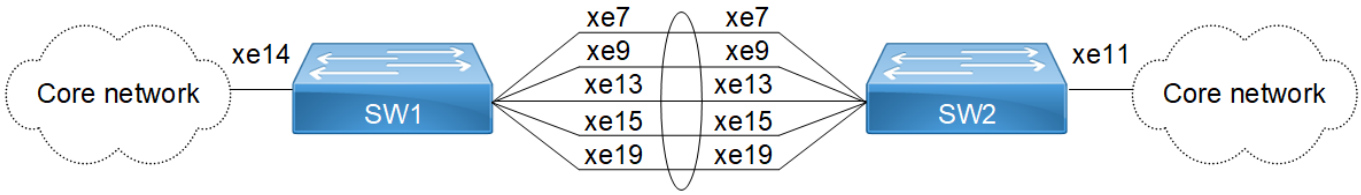


Figure 12-27: Port-Channel weight with dynamic LAG

SW1

`#configure terminal`	Enter configure mode.
`(config)#hostname SW1`	Configure host name
`(config)#bridge 1 protocol rstp vlan-bridge`	Create a RSTP VLAN bridge on customer side
`(config-vlan)#vlan database`	Enter VLAN database mode.
`(config-vlan)#vlan 2-100 bridge 1 state enable`	Configure VLAN for the bridge
`(config-vlan)#commit`	Commit the candidate configuration to the running configuration.
`(config-vlan)#exit`	Exit the VLAN configure mode.
`(config)#interface xe14`	Enter interface mode
`(config-if)#switchport`	Make interface as Switchport
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode hybrid`	Configure the mode as hybrid
`(config-if)#switchport hybrid allowed vlan all`	Configure allowed VLAN all on the interface
`(config-if)#commit`	Commit the candidate configuration to the running configuration.
`(config-if)#exit`	Exit the configure mode.

(config)#interface po1	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode hybrid	Configure the mode as hybrid
(config-if)#switchport hybrid allowed vlan all	Configure allowed vlan all for the hybrid mode
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe7	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1
(config-if)#port-channel weight 10	Configuring port-channel weight
(config-if)#exit	Exit interface mode.
(config)#interface xe9	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1
(config-if)#port-channel weight 2	Configuring port-channel weight
(config-if)#exit	Exit interface mode.
(config)#interface xe13	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1
(config-if)#port-channel weight 16	Configuring port-channel weight
(config-if)#exit	Exit interface mode.
(config)#interface xe15	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1
(config-if)#port-channel weight 5	Configuring port-channel weight
(config-if)#exit	Exit interface mode.
(config)#interface xe19	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1
(config-if)#port-channel weight 13	Configuring port-channel weight
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit the configure mode.

SW2

#configure terminal	Enter configure mode.
(config)#hostname SW2	Configure host name
(config)#bridge 1 protocol rstp vlan-bridge	Create a RSTP VLAN bridge on customer side
(config)#vlan database	Enter the VLAN database mode.
(config-vlan)#vlan 2-100 bridge 1 state enable	Configure VLAN for the bridge
(config-vlan)#commit	Commit the candidate configuration to the running configuration.
(config-vlan)#exit	Exit the VLAN configure mode.

(config)#interface xe11	Enter interface mode
(config-if)#switchport	Make interface as Switchport
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode hybrid	Configure the mode as hybrid
(config-if)#switchport hybrid allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface po1	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode hybrid	Configure the mode as hybrid
(config-if)#switchport hybrid allowed vlan all	Configure allowed vlan all for the hybrid mode
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe7	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1
(config-if)#exit	Exit interface mode.
(config)#interface xe9	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1
(config-if)#exit	Exit interface mode.
(config)#interface xe13	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1
(config-if)#exit	Exit interface mode.
(config)#interface xe15	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1
(config-if)#exit	Exit interface mode.
(config)#interface xe19	Enter interface mode
(config-if)#channel-group 1 mode active	Adding interface to channel-group 1
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit the configure mode.

Validation

As per the weights configured, traffic distribution will be happening across the member interfaces.

```
SW1#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 0001 - Oper Key 0001
     Link: xe7 (5008) weight: 10 sync: 1
     Link: xe9 (5010) weight: 2 sync: 1
```

```
     Link: xe13 (5014) weight: 16 sync: 1
     Link: xe15 (5016) weight: 5 sync: 1
     Link: xe19 (5020) weight: 13 sync: 1
SW1#show int counters rate mbps
+------------------+-------------+-------------+-------------+-------------+
|     Interface    |    Rx mbps  |    Rx pps   |    Tx mbps  |    Tx pps   |
+------------------+-------------+-------------+-------------+-------------+
 po1                0.00          0             280.03        50005
 xe7                0.00          0             61.02         10896
 xe8                0.00          0             0.00          0
 xe9                0.00          0             12.18         2175
 xe10               0.00          0             0.00          0
 xe12               0.00          0             0.00          0
 xe13               0.00          0             97.23         17361
 xe14               280.03        50004         0.00          0
 xe15               0.00          0             30.27         5405
 xe16               0.00          0             0.00          0
 xe18               0.00          0             0.00          0
 xe19               0.00          0             79.33         14166
SW1#
```

Port-Channel Weight with Static LAG

Topology

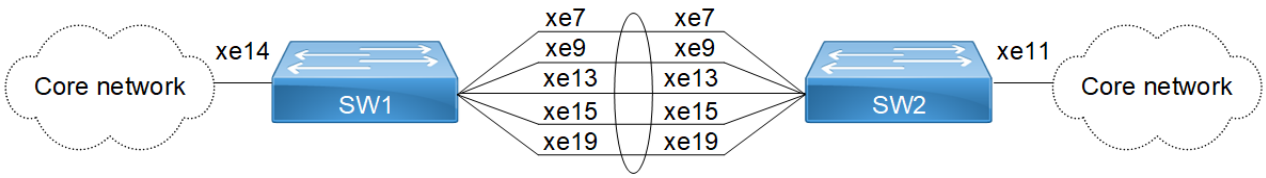


Figure 12-28: Figure 9-78: Port-channel weight with static LAG

SW1

`#configure terminal`	Enter configure mode.
`(config)#hostname SW1`	Configure host name
`(config)#bridge 1 protocol rstp vlan-bridge`	Create a RSTP VLAN bridge on customer side
`(config)#vlan database`	Enter VLAN database mode.
`(config-vlan)#vlan 2-100 bridge 1 state enable`	Configure VLAN for the bridge
`(config-vlan)#commit`	Commit the candidate configuration to the running configuration.
`(config-vlan)#exit`	Exit the VLAN configure mode.
`(config)#interface xe14`	Enter interface mode
`(config-if)#switchport`	Make interface as Switchport
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode hybrid`	Configure the mode as hybrid

(config-if)#switchport hybrid allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface sa1	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode hybrid	Configure the mode as hybrid
(config-if)#switchport hybrid allowed vlan all	Configure allowed vlan all for the hybrid mode
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe7	Enter interface mode
(config-if)#static-channel-group 1	Adding interface to static channel-group 1
(config-if)#port-channel weight 16	Configuring port-channel weight
(config-if)#exit	Exit interface mode.
(config)#interface xe9	Enter interface mode
(config-if)#static-channel-group 1	Adding interface to static channel-group 1
(config-if)#port-channel weight 14	Configuring port-channel weight
(config-if)#exit	Exit interface mode.
(config)#interface xe13	Enter interface mode
(config-if)#static-channel-group 1	Adding interface to static channel-group 1
(config-if)#port-channel weight 10	Configuring port-channel weight
(config-if)#exit	Exit interface mode.
(config)#interface xe15	Enter interface mode
(config-if)#static-channel-group 1	Adding interface to static channel-group 1
(config-if)#port-channel weight 8	Configuring port-channel weight
(config-if)#exit	Exit interface mode.
(config)#interface xe19	Enter interface mode
(config-if)#static-channel-group 1	Adding interface to static channel-group 1
(config-if)#port-channel weight 16	Configuring port-channel weight
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit the configure mode.

SW2

#configure terminal	Enter configure mode.
(config)#hostname SW2	Configure host name
(config)#bridge 1 protocol rstp vlan-bridge	Create a RSTP VLAN bridge on customer side
(config)#vlan database	Enter VLAN database mode.

(config-vlan)#vlan 2-100 bridge 1 state enable	Configure VLAN for the bridge
(config-vlan)#commit	Commit the candidate configuration to the running configuration.
(config-vlan)#exit	Exit the VLAN configure mode.
(config)#interface xe11	Enter interface mode
(config-if)#switchport	Make interface as Switchport
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode hybrid	Configure the mode as hybrid
(config-if)#switchport hybrid allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface sa1	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode hybrid	Configure the mode as hybrid
(config-if)#switchport hybrid allowed vlan all	Configure allowed vlan all for the hybrid mode
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit the configure mode.
(config)#interface xe7	Enter interface mode
(config-if)#static-channel-group 1	Adding interface to static channel-group 1
(config-if)#exit	Exit interface mode.
(config)#interface xe9	Enter interface mode
(config-if)#static-channel-group 1	Adding interface to static channel-group 1
(config-if)#exit	Exit interface mode.
(config)#interface xe13	Enter interface mode
(config-if)#static-channel-group 1	Adding interface to static channel-group 1
(config-if)#exit	Exit interface mode.
(config)#interface xe15	Enter interface mode
(config-if)#static-channel-group 1	Adding interface to static channel-group 1
(config-if)#exit	Exit interface mode.
(config)#interface xe19	Enter interface mode
(config-if)#static-channel-group 1	Adding interface to static channel-group 1
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit the configure mode.

Validation

As per the weights configured, traffic distribution will be happening across the member interfaces.

SW1

```
SW1#show static-channel-group
 Static Aggregator: sa1
 Member Status  weight
  xe7    up     16
  xe9    up     14
  xe13   up     10
  xe15   up     8
  xe19   up     16
SW1#show int counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 sa1                 0.00           0             280.03         50005
 xe7                 0.00           0             70.01          12501
 xe8                 0.00           0             0.00           0
 xe9                 0.00           0             61.27          10941
 xe10                0.00           0             0.00           0
 xe12                0.00           0             0.00           0
 xe13                0.00           0             43.80          7820
 xe14                280.03         50004         0.00           0
 xe15                0.00           0             34.95          6240
 xe16                0.00           0             0.00           0
 xe18                0.00           0             0.00           0
 xe19                0.00           0             70.01          12501
SW1#
```

CHAPTER 13 LACP Aggregator Force-up

Overview

Link Aggregation Control Protocol (LACP) facilitates the bundling of multiple physical interfaces into a single logical link, enhancing bandwidth and providing redundancy. Aggregator Force-Up extends LACP functionality by enabling links to be forced into an active state without successful LACP negotiation. This is crucial in environments where connected devices, such as servers during boot stages, might not support LACP or have temporary configuration limitations.

Feature Characteristics

- Allows all interfaces within a Link Aggregation Group (LAG) or MLAG to be manually set to an active state without requiring successful LACP negotiation.
- In force-up state, each physical interface in a LAG or MLAG acts as an independent bridge-port, handling MAC learning and L2 traffic independently rather than as part of the aggregated link.
- LACP agg force-up can be enabled in LAG or MLAG interface not in physical interface.
- Interfaces automatically transition out of force-up state and resume normal LACP-based operations when LACP communication is successfully established on any of the links.

Note:

- An LACP link configured with `force-up` enters the force-up state `90 seconds` after the parent LAG stops receiving LACP PDUs on all member links. The 90-second period is the `force-up activation delay timer`, which starts when the links transition to the `expiry or defaulted MUX state`.
- A force-up configured LACP link immediately exits the force-up state when the parent LAG interface receives LACP PDUs on any member link.
- The `force-up activation delay timer` restarts whenever a member LACP link in the parent LAG flaps.

Benefits

- Keeps network traffic flowing even when there’s a synchronization issue, preventing data loss and maintaining connectivity.
- Automatically switches the links to independent operation mode without manual intervention, simplifying network management.
- When synchronization is restored on any link, the LAG returns to its efficient, aggregated state.

LACP Aggregator Force-up for Dynamic LAG Configuration

Set up LACP Aggregator Force-Up to maintain network connectivity even when synchronization with the LACP partner is lost all member links in the LAG.

Topology

The provided topology diagram consists of a switch and a server (SW1 and server) connected to each other.

SW1: This the central switch in the topology. They are connected through two interfaces (xe1 and xe2).

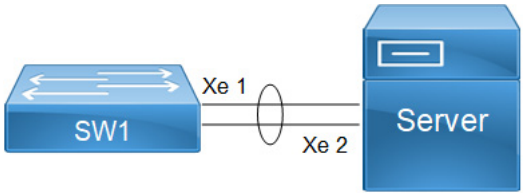


Figure 13-29: LACP Aggregator Force-up for Dynamic LAG

To configure LACP Aggregator Force-up for LAG on switch SW1 and Server, follow the steps:

1. Create VLANs and Bridge:
    1. Establish a bridge instance (`bridge 1`) with RSTP as the spanning tree protocol for VLAN-based bridging.
    2. Define VLANs 2 to 100 and associate it with (`bridge 1`) to enable the VLANs for bridging operations, and commit the changes.

```
SW1(config)# bridge 1 protocol rstp vlan-bridge
SW1(config)# vlan database
SW1(config-vlan)# vlan 2-100 bridge 1 state enable
SW1(config-vlan)# commit
SW1(config-vlan)# exit
```

2. Configure Port-channel Interface (`po1`) Aggregate Link between SW1 and Server:
    1. Enter configuration mode for Port-channel interface 1 (`po1`).
    2. Configure (`po1`) as a Layer 2 switchport.
    3. Associate (`po1`) with `bridge group 1` so that it operates within the defined bridging context.
    4. Set (`po1`) to trunk mode to carry traffic for multiple VLANs.
    5. Configure (`po1`) to carry traffic for all VLANs, facilitating communication across different VLANs within the network.
    6. Configure channel-group 1 for (`po1`) in active mode for LACP operation:

```
SW1(config)# interface po1
SW1(config-if)# switchport
SW1(config-if)# bridge-group 1
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk allowed vlan all
SW1(config-if)# commit
SW1(config-if)# exit
```

3. Configure the Interfaces (`xe1 and xe2`):
    1. Enter configuration mode for each interface (xe1 and xe2).
    2. Assign (`xe1` and `xe2`) to channel-group 1 to participate in the LACP bundle formed by po1, ensuring load balancing and redundancy across member links.

    Note: Follow similar steps for SW2, adjusting interface names and configurations accordingly to maintain consistency across the network.

```
SW1(config)# interface xe1
SW1(config-if)# channel-group 1 mode active
SW1(config-if)# exit
```

```
SW1(config)# interface xe2
SW1(config-if)# channel-group 1 mode active
SW1(config-if)# exit
```

4. Enable LACP Aggregator Force-Up on `po1`.

```
SW1(config)# interface po1
SW1(config-if)# lacp agg force-up
SW1(config-if)# commit
SW1(config-if)# exit
```

LACP Aggregator Force-up for MLAG Configuration

Set up LACP Aggregator Force-Up to maintain network connectivity even when synchronization with the LACP partner is lost on all member links in the MLAG.

Topology

This topology showcases a network setup designed to maximize redundancy, load balancing, and fault tolerance using MLAG and LACP with a Force-Up feature. The network is structured around top-of-rack switches (TOR1 and TOR2).

TOR1 and TOR2 operate as MLAG peers. This setup allows to appear as a single logical switch to connected device (Server).

Traffic can be distributed across the (TOR1 and TOR2), and if one switch fails, the other can handle the load without service interruption. The LACP Aggregator Force-Up feature is enabled to keep port channel member ports operationally up if all member links go down.

This ensures that the remains up, facilitating immediate traffic redirection and avoiding delays associated with LACP negotiation. Both TOR1 and TOR2 connect to server through multiple links, providing path redundancy.If any link or switch fails, the remaining links and switches maintain network connectivity and balance the load, thus avoiding single points of failure.

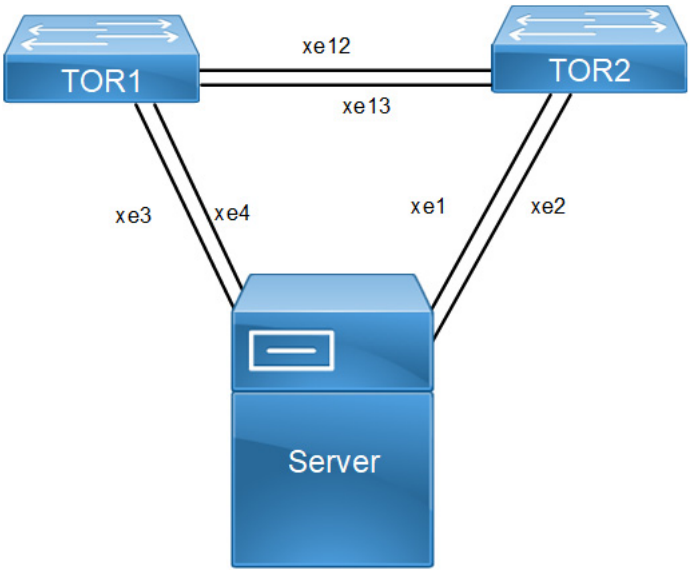


Figure 13-30: LACP Aggregator Force-up for MLAG

To configure LACP Aggregator Force-up for MLAG on switches TOR1, and TOR2, follow the steps:

1. Create VLANs and Bridge on TOR1,and TOR2:
    1. Establish a bridge instance (`bridge 1`) with RSTP as the spanning tree protocol for VLAN-based bridging.
    2. Define required vlans for example: VLANs 2 to 100 and associate it with (`bridge 1`) to enable the VLANs for bridging operations, and commit the changes.

```
TOR1(config)# bridge 1 protocol rstp vlan-bridge
TOR1(config)# vlan database
TOR1(config-vlan)# vlan 2-100 bridge 1 state enable
TOR1(config-vlan)# commit
TOR1(config-vlan)# exit
```

2. Configure Port Channels (`po`) as trunk ports allowing all VLANs, and commit the changes: For TORs: Configure interface `mlag1,po1,po3` as needed:
    1. Enter configuration mode for (`mlag1`).
    2. Configure (`mlag1)` as a Layer 2 switchport.
    3. Associate (`mlag1)` with `bridge group 1` so that it operates within the defined bridging context.
    4. Set (`mlag1)` to trunk mode to carry traffic for multiple VLANs.

```
TOR1(config)#interface mlag1
TOR1(config-if)#switchport
TOR1(config-if)#bridge-group 1
TOR1(config-if)#switchport mode trunk
TOR1(config-if)#switchport trunk allowed vlan all
TOR1(config-if)#mode active-active
TOR1(config-if)#commit
TOR1(config-if)#exit
```

    5. Configure po1 and map to mlag1.

```
TOR1(config)#interface po1
TOR1(config-if)#switchport
TOR1(config-if)#mlag 1
TOR1(config-if)#commit
```

    6. Configure po3.

```
TOR1(config)#interface po3
TOR1(config-if)#switchport
TOR1(config-if)#commit
```

3. Configure the Interfaces (For TOR1 `xe3, xe4, xe12, and xe13, and` For TOR2 `xe1, xe2, xe12, and xe13):`
    1. Enter configuration mode for each interface.
    2. Assign to channel-group 1 to participate in the LACP bundle formed by po1, ensuring load balancing and redundancy across member links.
    3. Configure as a Layer 2 switchport with trunk mode and allow all VLANs to facilitate communication across different VLANs within the network.

```
TOR1(config)#interface xe3
TOR1(config-if)#channel-group 1 mode active
TOR1(config-if)#exit
TOR1(config)#interface xe4
```

```
  TOR1(config-if)#channel-group 1 mode active
  TOR1(config-if)#commit
  TOR1(config-if)#exit
  TOR1(config)#interface xe12
  TOR1(config-if)#channel-group 3 mode active
  TOR1(config-if)#exit
  TOR1(config)#interface xe13
  TOR1(config-if)#channel-group 3 mode active
  TOR1(config-if)#commit
  TOR1(config Enable LACP Aggregator Force-up on MLAG interfaces in TOR1 and
TOR2:
TOR1(config)#interface mlag1
TOR1(config-if)#lacp agg force-up
TOR1(config-if)#commit
TOR1(config-if)#exit
```

Note: Similarly, follow the steps to configure `mlag1` for TOR2.

Configuration Snapshot

Dynamic LAG:

```
bridge 1 protocol rstp vlan-bridge
vlan database
 vlan 2-4000 bridge 1 state enable
!
interface po1
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 load-interval 30
 port-channel load-balance rtag7
 lacp agg force-up
!
interface xe1
 channel-group 1 mode active
!
interface xe2
 channel-group 1 mode active
!
 exit
```

MLAG:

```
bridge 1 protocol rstp vlan-bridge
vlan database
 vlan 2-4000 bridge 1 state enable
!
interface mlag1
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 load-interval 30
 lacp agg force-up
!
interface po1
```

```
 port-channel load-balance rtag7
 switchport
 mlag 1
!
interface po3
 switchport
 port-channel load-balance rtag7
!
interface xe3
 channel-group 1 mode active
!
interface xe4
 channel-group 1 mode active
!
interface xe12
 channel-group 3 mode active
!
interface xe13
 channel-group 3 mode active
!
 exit
!
mcec domain configuration
 domain-address 1111.2222.3333
 domain-system-number 1
 intra-domain-link po3
```

Dynamic LAG Validation

- Verify `agg force-up` is enabled in SW1.

```
SW1#show etherchannel summary
  Aggregator po1 100001
  Port-channel Force-Up Mode : Activated
  Aggregator Type: Layer2
  Admin Key: 0001 - Oper Key 0001
     Link: xe1 (5034) sync: 0 (agg-force-up)
     Link: xe2 (5035) sync: 0 (agg-force-up)
```

MLAG Validation

- Verify `agg force-up` is enabled in TOR1.

```
TOR1#show mlag domain summary

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number            : 1
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : po3
Domain Adjacency                : UP
```

```
MCEC PDU local version          : 1
MCEC PDU peer version           : 1
Domain Sync via                 : Intra-domain-interface
Peer SVI interface MAC Address : 5C.07.58.6F.83.5E

-----------------------------------
MLAG Configuration
-----------------------------------

MLAG-1
  Mapped Aggregator             : po1
  Physical properties Digest    : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6 22
  Total Bandwidth               : 0
  Mlag Sync                     : IN_SYNC
  Mode                          : Active-Active
  Current Mlag state            : Standby
  Aggregator Force-Up Mode      : Activated

TOR1#show etherchannel summary
  Aggregator po1 100001
  Mlag Force-Up Mode : Activated
  Aggregator Type: Layer2
  Parent Aggregator : Active mlag1
  Admin Key: 16385 - Oper Key 16385
     Link: xe3 (5004) sync: 0 (agg-force-up) (Mlag-active-link)
     Link: xe4 (5008) sync: 0 (agg-force-up) (Mlag-active-link)
-------------------------------------

  Aggregator po3 100003
  Aggregator Type: Layer2
  Admin Key: 0003 - Oper Key 0003
     Link: xe12 (5011) sync: 1
     Link: xe13 (5015) sync: 1
```

Implementation Examples

Dynamic Port-Channel configuration:

Both interfaces in the dynamic port-channel must support force-up to allow the server to boot using any connected link.

During the server's boot stage, the force-up feature ensures that any one of the connected interfaces can be used to initiate and complete the boot process, while the other interface remains inactive until LACP communication is established.

MLAG Configuration Requirement:

To support network booting, the MLAG domain is configured with LACP force-up. This allows at least one link to become active, ensuring the server can boot over the network.

Typically, all interfaces (`xe1, xe2, xe3, xe4`) need to be prepared to provide force-up capabilities to handle server booting flexibility.

Traffic Management:

When in force-up state, each interface operates as an individual bridge-port.

CLI Command

The LACP aggregator force-up feature introduces the `lacp agg force-up` configuration command.

lacp agg force-up

Use this command to configure Aggregator Force-up on Dynamic LAG or Dynamic MLAG interface.

If this command is enabled and LACP Partner sync is not established on any of the member links in Aggregator then, all the member links will enter Aggregator Force-up state in which they will act like individual bridge ports with respect to Layer2 Learning, Flooding, or Forwarding. Once LACP Partner sync is established on atleast one member link, the members will exit Aggregator Force-up and become part of the LAG that is normal LAG functioning is retained.

Use `no lacp agg force-up` parameter of this command to disable the aggregator force-up state.

Command Syntax

```
lacp agg force-up
no lacp agg force-up
```

Parameters

None

Default

Disabled

Command Mode

Interface mode

Applicability

Introduced the `lacp agg force-up` parameter in the OcNOS version 6.5.2.

Example

The following sequence of commands is used to configure the LACP Aggregator Force-Up feature in MLAG:

```
#configure terminal
(config)#interface mlag1
(config-if)#lacp agg force-up
(config-if)#exit
```

The following sequence of commands is used to configure the LACP Aggregator Force-Up feature in Dynamic LAG:

```
#configure terminal
(config)#interface po1
(config-if)#lacp agg force-up
(config-if)#exit
```

Glossary

The following provides definitions for key terms or abbreviations and their meanings used throughout this document:

Key Terms/Acronym	Description
Link Aggregation Control Protocol (LACP)	A protocol provides a way to bundle several physical ports together to form a single logical channel for the purpose of increasing bandwidth and providing redundancy.
Aggregator	A group of physical interfaces that are combined into a single logical interface (known as a port channel or link aggregation group) for load balancing and redundancy.
Aggregator Force-Up	A feature that keeps the members of LACP aggregator (port channel) operationally up, even if all member links are down. This is typically used in scenarios where there is server boot up.
Multi-Chassis Link Aggregation Group (MLAG)	Creation of a single logical link aggregation group across two separate switches, providing redundancy and load balancing across multiple chassis.
Port Channel (Po)	A logical grouping of multiple physical network interfaces, combined to act as a single interface. This allows for increased bandwidth and redundancy.
Active Mode	In LACP, active mode means the device actively initiates LACP negotiations and participates in the formation of LACP port channels.
Passive Mode	In LACP, passive mode means the device only responds to LACP packets but does not initiate the formation of LACP port channels.

CHAPTER 14 MLAG Configuration

Overview

This chapter contains a complete example of Multi-Chassis Link Aggregation (MLAG) configuration.

MLAG expands the concept of link aggregation so that it provides node-level redundancy by allowing two or more nodes to share a common LAG endpoint. It emulates multiple nodes to represent as a single logical node to the remote node running Link aggregation. As a result, even if one of the nodes is down there exists a path to reach the destination through the other nodes.

Note:

- MLAG is only compatible with VPWS.
- MLAG is supported only in Active-Standby mode.
- All MLAG nodes must have the same MAC table size - as specified by each node's switching ASIC forwarding profile limit.
- For multi-ASIC boards, performing measurements (as either sender or reflector) on LAG interfaces requires all LAG members to be located on the same ASIC.

The MLAG primary and secondary physical devices synchronize with each other to create a single logical domain called Multi-Chassis Ether Channel (MCEC) domain. The exchange of information between MLAG primary and secondary devices to maintain this MCEC domain can be done with the use of IDL and IDP.

Intra-Domain-Link (IDL)

This link is used by MLAG primary and secondary devices to synchronize the states between each other via MCEC packets to create the illusion of a single control plane. The MLAG peers use the IDL to exchange control information and coordinate with each other to ensure that data traffic is forwarded properly. The IDL interface is capable of carrying data traffic:

1. If a MLAG interface to which data traffic is destined is operationally down, the data traffic will be sent to MLAG peer device via IDL to avoid any loss.
2. If data traffic received on a MLAG device is destined for a host that is reachable via peer MLAG device only, then, the data traffic is sent over IDL to the peer MLAG device..

Intra-Domain-Peer (IDP)

This is an alternative way to synchronize the states between MLAG primary and secondary devices. In particular, it provides a Layer 3 communication path to carry MCEC packets. No data traffic is carried over the IDP. Hence, data traffic loss is expected, in case of MLAG interface failure.

Following are the possible types of interconnections for the IDP:

1. The `eth0` out-of-band management interface
2. It can be routed in-band over an L3 infrastructure

Options to Configure Intra-Domain

With IDL only

The IDL uses either a single physical or an aggregated ethernet interface. However, if IDL fails, the states between MLAG devices can no longer be synchronized. Configuring the IDL along with backup IDP provides more robustness during network disruptions.

Case-1: IDL Link Failure

- If strict Active-Standby is enabled: The standby node does not become active.
- If strict Active-Standby is disabled: The standby node becomes active, resulting in a split-brain (Active-Active) scenario.

Case-2: MLAG Active Device Failure/Reload

- If the device is reloaded by the admin via OcNOS commands: The standby node becomes active.
- If the device reboots due to any other reason:
  - If strict Active-Standby is enabled: The standby node does not become active.
  - If strict Active-Standby is disabled: The standby node becomes active.

With IDP only

The IDP without IDL can be used in cases where data traffic transmission between the primary and secondary MLAG devices are not needed.

Case 1: IDP link failure

- Behavior is the same as the With IDL only use case.

Case 2: MLAG active device Failure/Reload

- Behavior is the same as the With IDL only use case.

With IDL and IDP

When the IDL fails, the IDP (if configured) can be used as a backup mechanism to synchronize the states between MLAG peer devices. Also, it helps the MLAG switch to determine whether the IDL itself has failed or whether the peer MLAG device is operationally down. When both the IDL and IDP are configured, following are the behavior of the MLAG devices when the link/device fails:

Case-1: IDP Link failure

In this case, no impact on MLAG, therefore, no network downtime.

Case-2: IDL Link Failure

In this case, MCEC domain adjacency comes up via IDP. When the IDL link fails, MLAG Active-Active will be operational as MLAG Active-Standby (Safe Mode) to minimize network disruptions caused by Dual-Active (Split Brain) mode. It is expected that the traffic loss for hosts directly connected to the Standby device as data traffic cannot be carried over in the IDP.

Case-3: MLAG Peer Device Failure/Reload

When MLAG peer device reloads, MCEC domain adjacency goes down. The traffic is forwarded through the operational links in the Active MLAG device.

Case-4: Both IDL and IDP Failure

If both IDL and IDP link fails, Dual-Active (Split brain scenario) can be expected. There will be network instability/ disruption as both MLAG nodes are operating as Active-Active with MCEC Domain Adjacency down.

Topology

In the below example TOR1 and TOR2 forms a MLAG domain.

As shown in Figure 14-31, TOR1 and TOR2 forms a domain and thus provides the redundancy. Even if TOR1 or TOR2 is down, there exist a redundant path to forward the traffic.

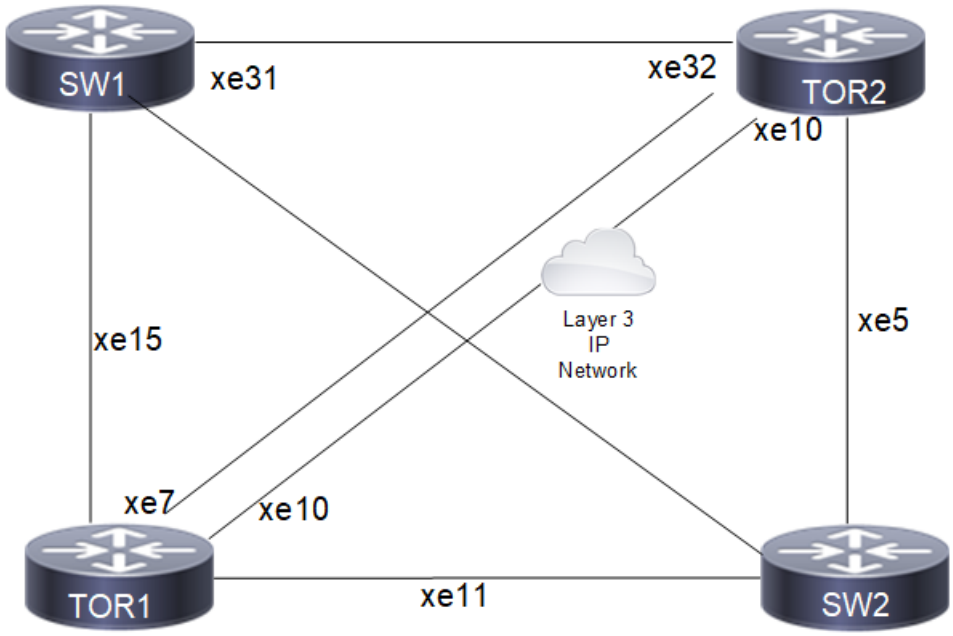


Figure 14-31: MLAG with IDL and IDP Topology

Configuration

Switch 1

`SW1#configure terminal`	Enter the config terminal.
`(config)#hostname SW1`	Assign the hostname for the router.
`SW1(config)#bridge 1 protocol rstp vlan-bridge`	Create bridge.
`SW1(config)#vlan database`	Enter the VLAN database.
`SW1(config-vlan)#vlan 2-1002 bridge 1 state enable`	Create the VLANs.
`SW1(config-vlan)#exit`	Exit the VLAN database.
`SW1(config)#int po1`	Enter the interface mode.
`SW1(config-if)#switchport`	Configure the interface as Layer 2.
`SW1(config-if)#bridge-group 1 spanning-tree disable`	Disable the spanning-tree for the interface.
`SW1(config-if)#bridge-group 1`	Assign the bridge to the interface.
`SW1(config-if)#switchport mode trunk`	Configure the interface as trunk mode.

SW1(config-if)#switchport trunk allowed vlan all	Configure the interface to allow all VLAN ids.
SW1(config-if)#load-interval 30	Configure load interval.
SW1(config-if)#mtu 9216	Set mtu value.
SW1(config-if)#mode active-active	Mode needs to be configured as active-active.
SW1(config-if)#exit	Exit the interface mode.
SW1(config)#int xe15	Enter the interface mode.
SW1(config-if)#channel-group 1 mode active	Add the interface as member of LAG interface.
SW1(config-if)#int xe31	Enter the interface mode.
SW1(config-if)#channel-group 1 mode active	Add the interface as member of LAG interface.
SW1(config-if)#commit	Commit the configure on the node.
SW1(config-if)#exit	Exit the interface mode.

TOR-1

TOR1#configure terminal	Enter the config terminal.
TOR1(config)#hostname TOR1	Assign the hostname for the router.
TOR1(config)#bridge 1 protocol rstp vlan-bridge	Create bridge.
TOR1(config)#vlan database	Enter the VLAN database.
TOR1(config-vlan)#vlan 2-1002 bridge 1 state enable	Create the VLANs.
TOR1(config-vlan)#exit	Exit the VLAN database.
TOR1(config)#int mlag1	Create the MLAG interface.
TOR1(config-if)#switchport	Configure the interface as Layer 2.
TOR1(config-if)#bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface.
TOR1(config-if)#bridge-group 1	Assign the bridge to the interface.
TOR1(config-if)#switchport mode trunk	Configure the interface as trunk mode.
TOR1(config-if)#switchport trunk allowed vlan all	Configure the interface to allow all VLAN ids.
TOR1(config-if)#load-interval 30	Configure load interval.
TOR1(config-if)#mtu 9216	Set mtu value.
TOR1(config-if)#mode active-active	Mode needs to be configured as active-active.
TOR1(config-if)#exit	Exit the interface mode.
TOR1(config)#int mlag2	Create the MLAG interface.
TOR1(config-if)#switchport	Configure the interface as Layer 2.
TOR1(config-if)#bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface.
TOR1(config-if)#bridge-group 1	Assign the bridge to the interface.
TOR1(config-if)#switchport mode trunk	Configure the interface as trunk mode.
TOR1(config-if)#switchport trunk allowed vlan all	Configure the interface to allow all VLAN ids.
TOR1(config-if)#load-interval 30	Configure load interval.

TOR1(config-if)#mtu 9216	Set mtu value.
TOR1(config-if)#mode active-active	Mode needs to be configured as active-active.
TOR1(config-if)#exit	Exit the interface mode.
TOR1(config)#int po1	Create the port channel interface.
TOR1(config-if)#switchport	Configure the interface as Layer 2.
TOR1(config-if)#mlag 1	Bind MLAG to the port channel.
TOR1(config-if)#exit	Exit the interface mode.
TOR1(config)#int po2	Create the port channel interface
TOR1(config-if)#switchport	Configure the interface as Layer 2.
TOR1(config-if)#mlag 2	Bind MLAG to the port channel.
TOR1(config-if)#exit	Exit the interface mode.
TOR1(config)#interface xe7	Configure xe7 interface mode only if the IDL is required.
TOR1(config-if)#switchport	Configure the interface as Layer 2 only if the IDL is required.
TOR1(config-if)#exit	Exit the interface mode.
TOR1(config-if)#interface xe10	Configure xe10 interface mode only if the IDP is required..
TOR1(config-if)#ip address 2.2.2.2/24	Configure source IP address for IDP only if the IDP is required.
TOR1(config)#int xe15	Enter the interface mode.
TOR1(config-if)#channel-group 1 mode active	Add the interface as member of LAG interface.
TOR1(config-if)#exit	Exit the interface mode.
TOR1(config)#int xe11	Enter the interface mode.
TOR1(config-if)#channel-group 2 mode active	Add the interface as member of LAG interface.
TOR1(config-if)#exit	Exit the interface mode.
TOR1(config)#mcec domain configuration	Enter the MCEC mode.
TOR1(config-mcec-domain)#domain-system-number 1	Assign the domain system number for MLAG interface.
TOR1(config-mcec-domain)#domain-address 1111.2222.3333	Assign the domain address.
TOR1(config-mcec-domain)#domain-hello-timeout short	Assign the domain hello timeout.
TOR1(config-mcec-domain)#intra-domain-link xe7	Assign the interface as IDL only if the IDP is required.
TOR1(config-mcec-domain)#)#intra-domain-peer 2.2.2.3 source-address 2.2.2.2	Configure source ip address for IDP only if the IDP is required.
TOR1(config-mcec-domain)#exit	Exit the MCEC domain.
TOR1(config-mcec-domain)#commit	Commit the configure on the node.
TOR1(config)#exit	Exit the config terminal.

TOR-2

TOR2#configure terminal	Enter the config terminal.
TOR2(config)#hostname TOR2	Assign the hostname for the router.
TOR2(config)#bridge 1 protocol rstp vlan-bridge	Create bridge.

`TOR2(config)#vlan database`	Enter the VLAN database.
`TOR2(config-vlan)#vlan 2-1002 bridge 1 state enable`	Create the VLANs.
`TOR2(config-vlan)#exit`	Exit the VLAN database.
`TOR2(config)#int mlag1`	Create the MLAG interface.
`TOR2(config-if)#switchport`	Configure the interface as Layer 2.
`TOR2(config-if)#bridge-group 1 spanning-tree disable`	Disable the spanning-tree for the interface.
`TOR2(config-if)#bridge-group 1`	Assign the bridge to the interface.
`TOR2(config-if)#switchport mode trunk`	Configure the interface as trunk mode.
`TOR2(config-if)#switchport trunk allowed vlan all`	Configure the interface to allow all VLAN ids.
`TOR2config-if)#load-interval 30`	Configure load interval.
`TOR2(config-if)#mtu 9216`	Set mtu value.
`TOR2(config-if)#mode active-active`	Mode needs to be configured as active-active.
`TOR2(config-if)#exit`	Exit the interface mode.
`TOR2(config)#int mlag2`	Create the MLAG interface.
`TOR2(config-if)#switchport`	Configure the interface as Layer 2.
`TOR2(config-if)#bridge-group 1 spanning-tree disable`	Disable the spanning-tree for the interface.
`TOR2(config-if)#bridge-group 1`	Assign the bridge to the interface.
`TOR2(config-if)#switchport mode trunk`	Configure the interface as trunk mode.
`TOR2(config-if)#switchport trunk allowed vlan all`	Configure the interface to allow all VLAN ids.
`TOR2config-if)#load-interval 30`	Configure load interval.
`TOR2(config-if)#mtu 9216`	Set mtu value.
`TOR2(config-if)#mode active-active`	Mode needs to be configured as active-active.
`TOR2(config-if)#exit`	Exit the interface mode.
`TOR2(config)#int po1`	Create the port channel interface
`TOR2(config-if)#switchport`	Configure the interface as Layer 2
`TOR2(config-if)#mlag 1`	Bind MLAG to the port channel.
`TOR2(config-if)#exit`	Exit the interface mode.
`TOR2(config)#int po2`	Create the port channel interface.
`TOR2(config-if)#switchport`	Configure the interface as Layer 2.
`TOR2(config-if)#mlag 2`	Bind MLAG to the port channel.
`TOR2(config-if)#exit`	Exit the interface mode.
`TOR2(config)#interface xe7`	Enter the interface mode
`TOR2(config-if)#switchport`	Configure the interface as Layer 2.
`TOR2(config-if)#interface xe10`	Enter the interface mode.
`TOR2(config-if)#ip address 2.2.2.3/24`	Configure source ip address for IDP only if the IDP is required.
`TOR2(config-if)#exit`	Exit the interface mode.
`TOR2(config)#int xe32`	Enter the interface mode.

TOR2(config-if)#channel-group 1 mode active	Add the interface as member of LAG interface.
TOR2(config-if)#exit	Exit the interface mode.
TOR2(config)#int xe5	Enter the interface mode
TOR2(config-if)#channel-group 2 mode active	Add the interface as member of LAG interface.
TOR2(config-if)#exit	Exit the interface mode.
TOR2(config)#mcec domain configuration	Enter the MCEC mode.
TOR2(config-mcec-domain)#domain-system-number 2	Assign the domain system number for MLAG interface.
TOR2(config-mcec-domain)#domain-address 1111.2222.3333	Assign the domain address.
TOR2(config-mcec-domain)#domain-hello-timeout short	Assign the domain hello timeout.
TOR2(config-mcec-domain)#intra-domain-link xe7	Assign the interface as IDL only if the IDL is required.
TOR2(config-mcec-domain)#)#intra-domain-peer 2.2.2.2 source-address 2.2.2.3	Configure source ip address for IDP only if the IDP is required.
TOR2(config-mcec-domain)#exit	Exit the MCEC domain.
TOR2(config-mcec-domain)#commit	Commit the configure on the node.
TOR2(config)#exit	Exit the config terminal.

Switch 2

SW2#configure terminal	Enter the config terminal.
SW2(config)#hostname SW2	Assign the hostname for the router.
SW2(config)#bridge 1 protocol rstp vlan-bridge	Create bridge.
SW2(config)#vlan database	Enter the VLAN database
SW2(config-vlan)#vlan 2-1002 bridge 1 state enable	Create the VLANs.
SW2(config-vlan)#exit	Exit the VLAN database
SW2(config)#int po2	Enter the interface mode
SW2(config-if)#switchport	Configure the interface as Layer 2
SW2(config-if)#bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface.
SW2(config-if)#bridge-group 1	Assign the bridge to the interface.
SW2(config-if)#switchport mode trunk	Configure the interface as trunk mode.
SW2(config-if)#switchport trunk allowed vlan all	Configure the interface to allow all VLAN ids.
SW2(config-if)#load-interval 30	Configure load interval.
SW2(config-if)#mtu 9216	Set mtu value.
SW2(config-if)#mode active-active	Mode needs to be configured as active-active.
SW2(config-if)#exit	Exit the interface mode.
SW2(config)#int xe11	Enter the interface mode.
SW2(config-if)#channel-group 2 mode active	Add the interface as member of LAG interface.
SW2(config-if)#int xe5	Enter the interface mode.

`SW2(config-if)#channel-group 2 mode active`	Add the interface as member of LAG interface.
`SW2(config-if)#commit`	Commit the configure on the node.
`SW2(config-if)#exit`	Exit the interface mode.

Validation

Switch 1

```
SW1#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 0001 - Oper Key 0001
     Link: xe15 (5015) sync: 1
     Link: xe31 (5031) sync: 0
SW1#

SW1#show etherchannel detail
 Aggregator po1 100001
 Aggregator Type: Layer2
  Mac address: 34:17:eb:e4:af:10
  Admin Key: 0001 - Oper Key 0001
   Actor LAG ID- 0x8000,34-17-eb-4b-af-00,0x0001
   Receive link count: 1 - Transmit link count: 1
   Individual: 0 - Ready: 1
  Partner LAG ID- 0x8000,11-11-22-22-33-33,0x4001
    Link: xe15 (5015) sync: 1
    Link: xe31 (5031) sync: 0
  Collector max delay: 5
SW1#
```

TOR 1

```
TOR1#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 16385 - Oper Key 16385
     Link: xe15 (5015) sync: 1 (Mlag-active-link)
-------------------------------------
  Aggregator po2 100002
  Aggregator Type: Layer2
  Admin Key: 16386 - Oper Key 16386
     Link: xe11 (5011) sync: 1 (Mlag-active-link)
TOR1#

TOR1#show mlag domain summary

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number            : 1
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : xe7
Source Address                  : 2.2.2.2
Intra-domain-peer               : 2.2.2.3
Domain Adjacency                : UP
```

```
MCEC PDU local version          : 1
MCEC PDU peer version           : 1
Domain Sync via                 : Intra-domain-interface
Peer SVI interface MAC Address : E8.C5.7A.69.4C.B3

-----------------------------------
MLAG Configuration
-----------------------------------

MLAG-1
  Mapped Aggregator             : po1
  Physical properties Digest    : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6
22

  Total Bandwidth               : 10g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active-Standby
  Current Mlag state            : Active
  Switchover-mode               : Revertive


MLAG-2
  Mapped Aggregator             : po2
  Physical properties Digest    : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6
22

  Total Bandwidth               : 10g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active-Standby
  Current Mlag state            : Active
  Switchover-mode               : Revertive

TOR1#

TOR1#show etherchannel detail
 Aggregator po1 100001
 Aggregator Type: Layer2
  Mac address: 3c:2c:99:1a:da:89
  Admin Key: 16385 - Oper Key 16385
   Actor LAG ID- 0x8000,11-11-22-22-33-33,0x4001
   Receive link count: 1 - Transmit link count: 1
   Individual: 0 - Ready: 1
  Partner LAG ID- 0x8000,34-17-eb-4b-af-00,0x0001
    Link: xe15 (5015) sync: 1 (Mlag-active-link)
  Collector max delay: 5
-------------------------------------------------
 Aggregator po2 100002
 Aggregator Type: Layer2
  Mac address: 3c:2c:99:1a:da:85
  Admin Key: 16386 - Oper Key 16386
   Actor LAG ID- 0x8000,11-11-22-22-33-33,0x4002
   Receive link count: 1 - Transmit link count: 1
   Individual: 0 - Ready: 1
  Partner LAG ID- 0x8000,3c-2c-99-c0-9f-79,0x0002
    Link: xe11 (5011) sync: 1 (Mlag-active-link)
  Collector max delay: 5
TOR1#
```

```
TOR1#show mcec statistics

Unknown MCCPDU received on the system            : 0

-----------------------------------
IDP                 : xe7
-----------------------------------
   Valid RX Hello PDUs                           : 4054
   Valid TX Hello PDUs                           : 4191
   Valid RX Info PDUs                            : 66
   Valid TX Info PDUs                            : 16

   Valid RX Mac Sync PDUs                        : 53
   Valid TX Mac Sync PDUs                        : 61

MLAG 1
  Valid RX Info PDUs                             : 9
  Valid TX Info PDUs                             : 8

MLAG 2
  Valid RX Info PDUs                             : 12
  Valid TX Info PDUs                             : 8
TOR1#
```

TOR 2

```
TOR2#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 32769 - Oper Key 16385
     Link: xe32 (5032) sync: 0 (Mlag-standby-link)
--------------------------------------
  Aggregator po2 100002
  Aggregator Type: Layer2
  Admin Key: 32770 - Oper Key 16386
     Link: xe5 (5005) sync: 0 (Mlag-standby-link)
TOR2#

TOR2#show etherchannel detail
 Aggregator po1 100001
 Aggregator Type: Layer2
  Mac address: 80:a2:35:c4:e9:73
  Admin Key: 32769 - Oper Key 16385
   Actor LAG ID- 0x8000,11-11-22-22-33-33,0x4001
   Receive link count: 0 - Transmit link count: 0
   Individual: 0 - Ready: 1
  Partner LAG ID- 0x8000,34-17-eb-4b-af-00,0x0001
    Link: xe32 (5032) sync: 0 (Mlag-standby-link)
  Collector max delay: 5
-------------------------------------------------
 Aggregator po2 100002
 Aggregator Type: Layer2
  Mac address: 80:a2:35:c4:e9:58
  Admin Key: 32770 - Oper Key 16386
   Actor LAG ID- 0x8000,11-11-22-22-33-33,0x4002
   Receive link count: 0 - Transmit link count: 0
```

```
   Individual: 0 - Ready: 1
  Partner LAG ID- 0x8000,3c-2c-99-c0-9f-79,0x0002
    Link: xe5 (5005) sync: 0 (Mlag-standby-link)
  Collector max delay: 5
TOR2#
TOR2#
TOR2#show mlag domain summary

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number            : 2
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : xe7
Source Address                  : 2.2.2.3
Intra-domain-peer               : 2.2.2.2
Domain Adjacency                : UP
MCEC PDU local version          : 1
MCEC PDU peer version           : 1
Domain Sync via                : Intra-domain-interface
Peer SVI interface MAC Address : 80.A2.35.3A.40.94

-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator            : po1
  Physical properties Digest   : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6
22

  Total Bandwidth              : 10g
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Standby
  Current Mlag state           : Standby
  Switchover-mode              : Revertive


MLAG-2
  Mapped Aggregator            : po2
  Physical properties Digest   : 54 a9 3a 2a 2b 50 65 bb 3c bc 3d bd c2 43 d6
22

  Total Bandwidth              : 10g
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Standby
  Current Mlag state           : Standby
  Switchover-mode              : Revertive


TOR2#


TOR2#show mcec statistics
```

```
Unknown MCCPDU received on the system            : 0

-------------------------------------
IDP                 : xe7
-------------------------------------

  Valid RX Hello PDUs                           : 4177
   Valid TX Hello PDUs                           : 4159
   Valid RX Info PDUs                            : 16
   Valid TX Info PDUs                            : 66

   Valid RX Mac Sync PDUs                        : 74
   Valid TX Mac Sync PDUs                        : 30

MLAG 1
  Valid RX Info PDUs                            : 8
  Valid TX Info PDUs                            : 27

MLAG 2
  Valid RX Info PDUs                            : 8
  Valid TX Info PDUs                            : 39
TOR2#
```

Switch 2

```
SW2#show etherchannel summary
  Aggregator po2 100002
  Aggregator Type: Layer2
  Admin Key: 0002 - Oper Key 0002
     Link: xe5 (5005) sync: 0
     Link: xe11 (5011) sync: 1

SW2#show etherchannel detail
 Aggregator po2 100002
 Aggregator Type: Layer2
  Mac address: 3c:2c:99:26:e6:7f
  Admin Key: 0002 - Oper Key 0002
   Actor LAG ID- 0x8000,3c-2c-99-c0-9f-79,0x0002
   Receive link count: 1 - Transmit link count: 1
   Individual: 0 - Ready: 1
  Partner LAG ID- 0x8000,11-11-22-22-33-33,0x4002
    Link: xe5 (5005) sync: 0
    Link: xe11 (5011) sync: 1
  Collector max delay: 5
SW2#
```

MLAG Active-Active Dynamic Configuration

MLAG (also called DRNI, Distributed Resilient Network Interconnect) expands the concept of link aggregation so that it provides node-level redundancy by allowing two or more nodes to share a common LAG endpoint. MLAG emulates multiple nodes to represent as a single logical node to the remote node running link aggregation. As a result, even if one of the nodes is down there exists a path to reach the destination through the other nodes.

Note: MLAG is compatible only with a RSTP VLAN-aware bridge or a spanning tree disabled bridge.

Note: All MLAG nodes must have the same MAC table size as specified by each node's switching ASIC forwarding profile limit.

Topology

As shown in Figure 14-32, TOR 1 and TOR 2 form an MLAG domain. TOR 1 and TOR 2 are a single logical switch to LEAF and LwSW. Even if either TOR 1 or TOR 2 is down, there exists a path to reach other destinations.

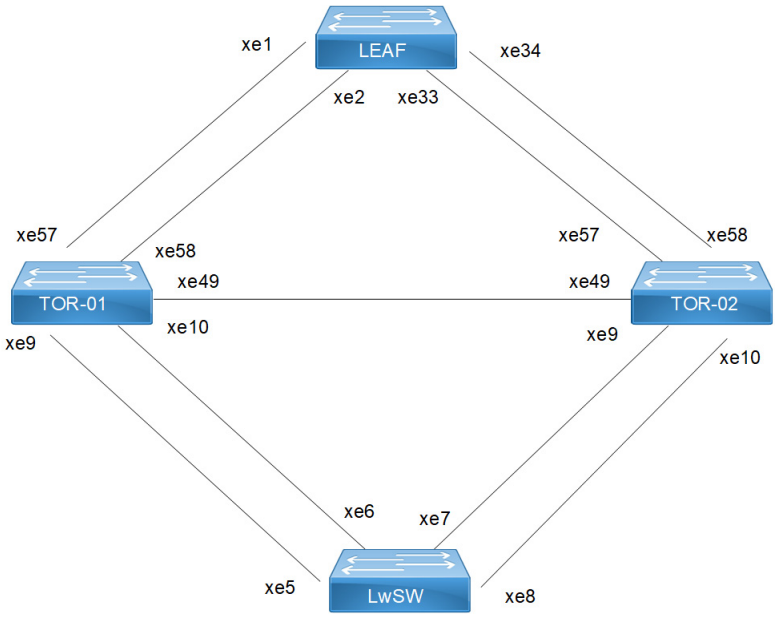


Figure 14-32: MLAG Active-Active Topology

LEAF

`#configure terminal`	Enter configure mode.
`(config)#hardware-profile filter egress-l2 enable`	Enable the hardware-profile filter
`(config)#bridge 1 protocol rstp vlan-bridge`	Create RSTP bridge 1.
`(config)#vlan 2 bridge 1 state enable`	Create VLAN 2.
`(config)#interface po2`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as Layer 2
`(config-if)#bridge-group 1 spanning-tree disable`	Disable the spanning-tree for the interface.
`(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`(config-if)#switchport trunk allowed vlan all`	Enable all VLAN identifiers on this interface.
`(config-if)#load-interval 30`	Configure load interval.
`(config-if)#mtu 9216`	Set mtu value.
`(config-if)#mode active-active`	Mode needs to be configured as active-active.

(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe33	Enter interface mode.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe34	Enter interface mode.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.

LwSW

#configure terminal	Enter configure mode.
(config)#hardware-profile filter egress-l2 enable	Enable the hardware-profile filter
(config)#bridge 1 protocol rstp vlan-bridge	Create RSTP bridge 1.
(config)#vlan 2 bridge 1 state enable	Create VLAN 2.
(config)#interface po1	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.

(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#load-interval 30	Configure load interval.
(config-if)#mtu 9216	Set mtu value.
(config-if)#mode active-active	Mode needs to be configured as active-active.
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit interface mode.
(config)#interface xe5	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe6	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe7	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe8	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.

TOR-01

#configure terminal	Enter configure mode.
(config)#hardware-profile filter egress-l2 enable	Enable the hardware-profile filter
(config)#interface mlag1	Enter interface mode.
(config-if)#mode active-active	Mode need to be configured as active-active
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface mlag2	Enable the hardware-profile filter
(config-if)#mode active-active	Mode need to be configured as active-active

(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#bridge 1 protocol rstp vlan-bridge	Create RSTP bridge 1.
(config)#vlan 2 bridge 1 state enable	Create VLAN 2.
(config)#interface mlag1	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface mlag2	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface po1	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#mlag 1	Enabling MLAG group number
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface po2	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#mlag 2	enabling Mlag group number
(config-if)#exit	Exit interface mode.
(config)#interface xe9	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe57	Enter interface mode.

(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe58	Enter interface mode.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe10	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe49	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#exit	Exit interface mode.
(config)#mcec domain configuration	Entering MCEC mode
(config-mcec-domain)#domain-address 1111.2222.3333	Domain address for the mlag domain
(config-mcec-domain)#intra-domain link xe49	Intra domain line between mlag domain
(config-mcec-domain)#domain-system-number 1	Number to identify the node in a domain
(config-mcec-domain)#commit	Commit the candidate configuration to the running configuration
(config-mcec-domain)#exit	Exit MCEC mode

TOR-02

#configure terminal	Enter configure mode.
(config)#hardware-profile filter egress-l2 enable	Enable the hardware-profile filter
(config)#interface mlag1	Enter interface mode.
(config-if)#mode active-active	Mode need to be configured as active-active
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode
(config)#interface mlag2	Enable the hardware-profile filter
(config-if)#mode active-active	Mode need to be configured as active-active
(config-if)#commit	Commit the candidate configuration to the running configuration

(config-if)#exit	Exit interface mode
(config)#bridge 1 protocol rstp vlan-bridge	Create RSTP bridge 1.
(config)#vlan 2 bridge 1 state enable	Create VLAN 2.
(config)#interface mlag1	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode
(config)#bridge 1 protocol rstp vlan-bridge	Create RSTP bridge 1.
(config)#vlan 2 bridge 1 state enable	Create VLAN 2.
(config)#interface mlag1	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface mlag2	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface po1	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#mlag 1	Enabling Mlag group number
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface po2	Enter interface mode.

(config-if)#switchport	Configure the interface as Layer 2
(config-if)#mlag 2	enabling MLAG group number
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe9	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe10	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe57	Enter interface mode.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe58	Enter interface mode.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#interface xe49	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit interface mode.
(config)#mcec domain configuration	Entering MCEC mode
(config-mcec-domain)#domain-address 1111.2222.3333	Domain address for the Mlag domain
(config-mcec-domain)#intra-domain link xe49	Intra domain Link between Mlag domains
(config-mcec-domain)#domain-system-number 2	Number to identify the node in domain
(config-mcec-domain)#exit	Exit MCEC mode
(config-mcec-domain)#commit	Commit the candidate configuration to the running configuration

Validation

```
#sh mlag domain details

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number           : 1
Domain Address                 : 1111.2222.3333
Domain Priority                : 1000
Intra Domain Interface         : xe49

Hello RCV State                : Current
Hello Periodic Timer State     : Fast Periodic
Domain Sync                    : IN_SYNC
Neigh Domain Sync              : IN_SYNC
Domain Adjacency               : UP

-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator           : po1
  Admin Key                   : 16385
  Oper Key                    : 16385
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

  Neigh Admin Key             : 32769
  Neigh Physical Digest       : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Info RCV State              : Current
  Info Periodic Time State    : Standby
  Mlag Sync                   : IN_SYNC
  Mode                        : Active-Active
  Current Mlag State          : Active


MLAG-2
  Mapped Aggregator           : po2
  Admin Key                   : 16386
  Oper Key                    : 16386
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

  Neigh Admin Key             : 32770
  Neigh Physical Digest       : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Info RCV State              : Current
  Info Periodic Time State    : Standby
  Mlag Sync                   : IN_SYNC
  Mode                        : Active-Active
```

```
  Current Mlag State          : Active


#sh etherchannel summary
% Aggregator po1 0
% Aggregator Type: Layer2
% Admin Key: 16385 - Oper Key 16385
%   Link: xe57 (5057) sync: 1 (Mlag-active-link)
%   Link: xe58 (5058) sync: 1 (Mlag-active-link)
% Aggregator po2 0
% Aggregator Type: Layer2
% Admin Key: 16386 - Oper Key 16386
%   Link: xe9 (5009) sync : 1 (Mlag-active-link)
%   Link: xe10 (5010) sync: 1 (Mlag-active-link)

#sh mlag 1 detail

MLAG-1
  Mapped Aggregator           : po1
  Admin Key                   : 16385
  Oper Key                    : 16385
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

  Neigh Admin Key             : 32769
  Neigh Physical Digest       : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Info RCV State              : Current
  Info Periodic Time State    : Standby
  Total Bandwidth             : 20g
  Mlag Sync                   : IN_SYNC
  Mode                        : Active-Active
  Current Mlag State          : Active


sh mcec statistics

Unknown MCCPDU received on the system            : 0

-------------------------------------
IDP xe49
-------------------------------------
   Valid RX Hello PDUs                          : 398
   Valid TX Hello PDUs                          : 417
   Valid RX Info PDUs                           : 16
   Valid TX Info PDUs                           : 6

   Valid RX Mac Sync PDUs                       : 3
   Valid TX Mac Sync PDUs                       : 4

MLAG 1
  Valid RX Info PDUs                            : 8
```

```
  Valid TX Info PDUs                          : 3

MLAG 2
  Valid RX Info PDUs                          : 8
  Valid TX Info PDUs                          : 3
sh mlag domain summary

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number            : 1
Domain Address                  : 1111.2222.3333
Domain Priority                 : 1000
Intra Domain Interface          : xe49
Domain Adjacency                : UP

-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator           : po1
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Total Bandwidth             : 40g
  Mlag Sync                   : IN_SYNC
  Mode                        : Active-Active
  Current Mlag State          : Active


MLAG-2
  Mapped Aggregator           : po2
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Total Bandwidth             : 40g
  Mlag Sync                   : IN_SYNC
  Mode                        : Active-Active
  Current Mlag State          : Active
```

Static Configuration

Static MLAG provides node-level redundancy by allowing two or more nodes in the network to share a common static-LAG endpoint. It emulates multiple nodes to represent as a single logical node to the remote node having static Link aggregation. As a result, even if one of the nodes is down there exists a path to reach the destination via other nodes.

Topology

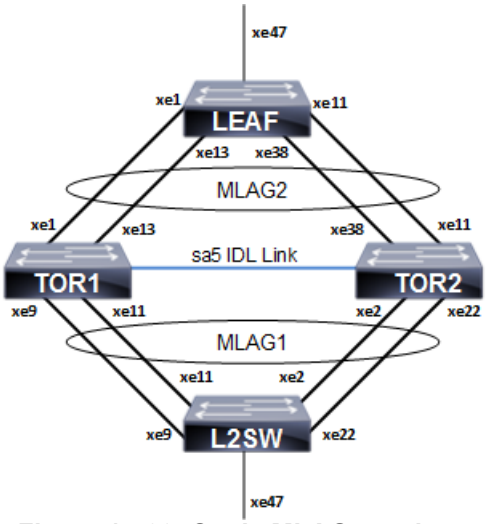


Figure 14-33: Static MLAG topology

L2SW

`#configure terminal`	Enter configure mode.
`(config)#hostname L2SW`	Configuring host name
`(config)#bridge 1 protocol rstp vlan-bridge`	Create a RSTP VLAN bridge on customer side
`(config)#vlan 2 bridge 1 state enable`	Configure VLAN for the bridge
`(config)#interface sa1`	Enter the interface mode
`(config-if)#bridge-group 1 spanning-tree disable`	Disable the spanning-tree for the interface
`(config-if)#switchport mode hybrid`	Configure the mode as hybrid
`(config-if)#switchport hybrid allowed vlan all`	Configure allowed VLAN all on the interface
`(config-if)#exit`	Exit the interface mode
`(config)#interface xe2`	Enter the interface mode
`(config-if)#static-channel-group 1`	Map static channel to the interface
`(config-if)#exit`	Exit the interface mode
`(config)#interface xe9`	Enter the interface mode
`(config-if)#static-channel-group 1`	Map static channel to the interface
`(config-if)#exit`	Exit the interface mode
`(config)#interface xe11`	Enter the interface mode
`(config-if)#static-channel-group 1`	Map static channel to the interface
`(config-if)#exit`	Exit the interface mode
`(config)#interface xe22`	Enter the interface mode
`(config-if)#static-channel-group 1`	Map static channel to the interface
`(config-if)#exit`	Exit the interface mode
`(config)#interface xe47`	Enter the interface mode
`(config-if)#switchport`	Make the interface as switch port

(config-if)#bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface
(config-if)#switchport mode hybrid	Configure the mode as hybrid
(config-if)#switchport hybrid allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#exit	Exit the interface mode

TOR1

#configure terminal	Enter configure mode.
(config)#hostname TOR1	Configuring host name
(config)#bridge 1 protocol provider-rstp edge	Create a PROVIDER-RSTP EDGE bridge
(config)#vlan 2 bridge 1 state enable	Configure VLAN for the bridge
(config)#vlan 200 type service point-point bridge 1 state enable	Configure SVLAN for the bridge
(config)#cvlan registration table map1 bridge 1	Configure CVLAN-SVLAN mapping registration table for the bridge
(config-cvlan-registration)#cvlan 2 svlan 200	Map CVLAN to SVLAN
(config-cvlan-registration)#exit	Exit the config-cvlan-registration mode
(config)#interface mlag1	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode customer-edge hybrid	Configure the mode as customer-edge hybrid
(config-if)#switchport customer-edge hybrid allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#switchport customer-edge vlan registration map1	Map the CVLAN registration table into the MLAG interface
(config-if)#mode active-standby	Configuring MLAG mode
(config-if)#exit	Exit the interface mode
(config)#interface mlag2	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-.if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode provider-network	Configure the mode as provider-network
(config-if)#switchport provider-network allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#mode active-standby	Configuring MLAG mode
(config-if)#exit	Exit the interface mode
(config)#interface sa1	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#mlag 1	Map MLAG on SA interface

(config-if)#exit	Exit the interface mode
(config)#interface sa2	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#mlag 2	Map MLAG on SA interface
(config-if)#exit	Exit the interface mode
(config)#interface xe1	Enter the interface mode
(config-if)#static-channel-group 2	Map static channel-group to the interface
(config-if)#exit	Exit the interface mode
(config)#interface xe13	Enter the interface mode
(config-if)#static-channel-group 2	Map static channel-group to the interface
(config-if)#exit	Exit the interface mode
(config)#interface xe9	Enter the interface mode
(config-if)#static-channel-group 1	Map static channel-group to the interface
(config-if)#exit	Exit the interface mode
(config)#interface xe11	Enter the interface mode
(config-if)#static-channel-group 1	Map static channel to the interface
(config-if)#exit	Exit the interface mode
(config)#interface sa5	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#exit	Exit the interface mode
(config)#interface xe3	Enter the interface mode
(config-if)#static-channel-group 5	Map static channel-group to the interface
(config)#interface xe5	Enter the interface mode
(config-if)#static-channel-group 5	Map static channel-group to the interface
(config-if)#exit	Exit the interface mode
(config)#mcec domain configuration	Enter the MLAG domain configuration mode
(config-mcec-domain)#domain-address 1111.2222.3333	Configure the MLAG domain address
(config-mcec-domain)#domain-system-number 1	Configure MLAG domain system number
(config-mcec-domain)#intra-domain-link sa5	Configure the intra domain link

TOR2

#configure terminal	Enter configure mode.
(config)#hostname TOR2	Configuring host name
(config)#bridge 1 protocol provider-rstp edge	Create a PROVIDER-RSTP EDGE bridge
(config)#vlan 2 bridge 1 state enable	Configure VLAN for the bridge
(config)#vlan 200 type service point-point bridge 1 state enable	Configure SVLAN for the bridge
(config)#cvlan registration table map1 bridge 1	Configure CVLAN-SVLAN mapping registration table for the bridge

(config-cvlan-registration)#cvlan 2 svlan 200	Map CVLAN to SVLAN
(config-cvlan-registration)#exit	Exit the config-CVLAN-registration mode
(config)#interface mlag1	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode customer-edge hybrid	Configure the mode as customer-edge hybrid
(config-if)#switchport customer-edge hybrid allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#switchport customer-edge vlan registration map1	Map the CVLAN registration table into the MLAG interface
(config-if)#mode active-standby	Configuring MLAG mode
(config-if)#exit	Exit the interface mode
(config)#interface mlag2	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode provider-network	Configure the mode as provider-network
(config-if)#switchport provider-network allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#mode active-standby	Configuring MLAG mode
(config-if)#exit	Exit the interface mode
(config)#interface sa1	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#mlag 1	Map MLAG on SA interface
(config-if)#exit	Exit the interface mode
(config)#interface sa2	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#mlag 2	Map MLAG on SA interface
(config-if)#exit	Exit the interface mode
(config)#interface xe11	Enter the interface mode
(config-if)#static-channel-group 2	Map static channel to the interface
(config-if)#exit	Exit the interface mode
(config)#interface xe38	Enter the interface mode
(config-if)#static-channel-group 2	Map static channel to the interface
(config-if)#exit	Exit the interface mode
(config)#interface xe2	Enter the interface mode
(config-if)#static-channel-group 1	Create static channel group
(config-if)#exit	Exit the interface mode
(config)#interface xe22	Enter the interface mode
(config-if)#static-channel-group 1	Create static channel group

(config-if)#exit	Exit the interface mode
(config)#interface sa5	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#exit	Exit the interface mode
(config)#interface xe3	Enter the interface mode
(config-if)#static-channel-group 5	Map static channel-group to the interface
(config)#interface xe5	Enter the interface mode
(config-if)#static-channel-group 5	Enter the interface mode
(config-if)#exit	Exit the interface mode
(config)#mcec domain configuration	Enter the MLAG domain configuration mode
(config-mcec-domain)#domain-address 1111.2222.3333	Configure the MLAG domain address
(config-mcec-domain)#domain-system-number 2	Configure MLAG domain system number
(config-mcec-domain)#intra-domain-link sa5	Configure the intra domain link
(config-if)#exit	Exit the interface mode

LEAF

#configure terminal	Enter configure mode.
(config)#hostname LEAF	Configuring host name
(config)#bridge 1 protocol provider-rstp edge	Create a PROVIDER-RSTP EDGE bridge
(config)#vlan 2 bridge 1 state enable	Configure VLAN for the bridge
(config)#vlan 200 type service point-point bridge 1 state enable	Configure SVLAN for the bridge
(config)#cvlan registration table map1 bridge 1	Configure CVLAN-SVLAN mapping registration table for the bridge
(config-cvlan-registration)#cvlan 2 svlan 200	Map CVLAN to SVLAN
(config-cvlan-registration)#exit	Exit the config-CVLAN-registration mode
(config)#interface sa2	Enter the interface mode
(config-if)#swtichport	Make the interface a switch port
(config-if)#bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface
(config-if)#switchport mode provider-network	Configure the mode as provider-network
(config-if)#)#switchport provider-network allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#exit	Exit the interface mode
(config)#interface xe1	Enter the interface mode
(config-if)#static-channel-group 2	Map the interface to the static channel-group
(config-if)#exit	Exit the interface mode
(config)#interface xe13	Enter the interface mode
(config-if)#static-channel-group 2	Create static channel group

(config-if)#exit	Exit the interface mode
(config)#interface xe11	Enter the interface mode
(config-if)#static-channel-group 2	Map the interface to the static channel-group
(config-if)#exit	Exit the interface mode
(config)#interface xe38	Enter the interface mode
(config-if)#static-channel-group 2	Create static channel group
(config-if)#exit	Exit the interface mode
(config)#interface xe47	Enter the interface mode
(config-if)#switchport	Make the interface as switch port
(config-if)#bridge-group 1 spanning-tree disable	Disable the spanning-tree for the interface
(config-if)#switchport mode customer-edge hybrid	Configure the mode as customer-edge hybrid
(config-if)#switchport customer-edge hybrid allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#switchport customer-edge vlan registration map1	Map the CVLAN registration table into the MLAG interface
(config-if)#exit	Exit the interface mode

Validation

```
TOR1#show mlag 1 detail

MLAG-1
Mapped Aggregator: sa1
Admin Key: 16385
Oper Key: 16385
Physical properties Digest: d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57 cc

Neigh Admin Key: 32769
Neigh Physical Digest: d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57 cc Info RCV State: Current
Info Periodic Time State: Standby Total Bandwidth: 40g
Mlag Sync: IN_SYNC
Mode: Active-Standby
Current Mlag State: Active
```

Switchover-mode: Revertive TOR1#

```
TOR1#show mlag domain summary


DomainConfiguration

Domain
System Number:
1
DomainAddress:1111.2222.3333
DomainPriority:32768
Intra Domain Interface: sa5
```

```
Domain Adjacency: UP
```

MLAG Configuration

MLAG-1

```
Mapped Aggregator: sa1
Physical properties Digest: d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57 cc Total
Bandwidth: 40g
Mlag Sync: IN_SYNC
Mode: Active-Standby
Current Mlag State: Active
Switchover-mode: Revertive
```

MLAG-2

```
Mapped Aggregator: sa2
Physical properties Digest: ae 56 a1 c5 b9 dc 46 a4 5d 97 dc 79 9c 6f a5 c8

Total Bandwidth: 40g
Mlag Sync: IN_SYNC
Mode: Active-Standby
Current Mlag State: Active
Switchover-mode: Revertive

TOR1#show mlag domain detail

Domain Configuration
DomainSystem Number:1
DomainAddress:1111.2222.3333
DomainPriority:32768
IntraDomain Interface:sa5

Hello RCV State: Current Hello Periodic Timer State: Slow Periodic Domain Sync: IN_SYNC
Neigh Domain Sync: IN_SYNC
Domain Adjacency: UP
```

MLAG Configuration

MLAG-1

```
Mapped Aggregator: sa1
Admin Key: 16385
Oper Key: 16385
Physical properties Digest: d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57 cc

Neigh Admin Key: 32769
Neigh Physical Digest: d a6 26 2d fa 9a 5c 7b e6 15 79 c2 d5 9c 57 cc Info RCV State:
Current
Info Periodic Time State: Standby Total Bandwidth: 40g
Mlag Sync: IN_SYNC
Mode: Active-Standby
Current Mlag State: Active Switchover-mode: Revertive
```

MLAG-2

```
Mapped Aggregator: sa2
Admin Key: 16386
Oper Key: 16386
Physical properties Digest: ae 56 a1 c5 b9 dc 46 a4 5d 97 dc 79 9c 6f a5 c8


Neigh Admin Key: 32770
Neigh Physical Digest: ae 56 a1 c5 b9 dc 46 a4 5d 97 dc 79 9c 6f a5 c8

Info RCV State: Current Info Periodic Time State : Standby Total Bandwidth: 40g
Mlag Sync: IN_SYNC
Mode: Active-Standby
Current Mlag State: Active Switchover-mode: Revertive
```

ARP ACL Configuration

Topology

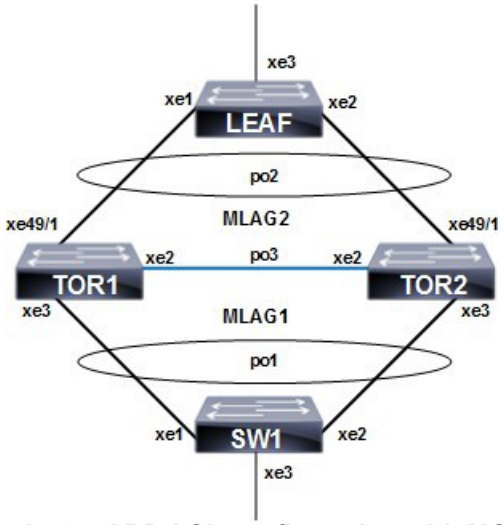


Figure 14-34: ARP ACL configuration with MC LAG

TOR1

`#configure terminal`	Enter configure mode.
`TOR1(config)#bridge 1 protocol provider-rstp edge`	Create provider RSTP bridge
`TOR1(config)#vlan 2-3990 type customer bridge 1 state enable`	Enable customer VLAN for bridge
`TOR1(config)#vlan 2-3990 type service point-point bridge 1 state enable`	Enable service VLAN for bridge
`TOR1(config)#cvlan registration table map1 bridge 1`	Create registration table

TOR1(config-cvlan-registration)#cvlan 2-3990 svlan 3990	Map CVLAN to svlan
TOR1(config-cvlan-registration)#exit	Exit the CVLAN registration table mode
TOR1(config-if)#interface mlag1	Enter MLAG interface
TOR1(config-if)#switchport	Configure interface as switchport
TOR1(config-if)#exit	Exit the interface mode
TOR1(config)#interface mlag2	Enter MLAG interface
TOR1(config-if)#switchport	Configure interface as switchport
TOR1(config-if)#bridge-group 1	Associate the interface with bridge group 1
TOR1(config-if)#switchport mode provider-network	Set the switching characteristics of this interface to provider network
TOR1(config-if)#switchport provider-network allowed vlan all	Set the switching characteristics of this interface to provider network and allow all VLAN
TOR1(config-if)#exit	Exit the interface mode
TOR1(config)#interface po1	Enter dynamic LAG interface
TOR1(config-if)#switchport	Configure interface as switchport
TOR1(config-if)#mlag 1	Enable MLAG group number
TOR1(config-if)#exit	Exit the interface mode
TOR1(config-if)#interface po2	Enter dynamic LAG interface
TOR1(config-if)#switchport	Configure interface as switchport
TOR1(config-if)#mlag 2	Enable MLAG group number
TOR1(config-if)#exit	Exit the interface mode
TOR1(config)#interface po3	Enter dynamic LAG interface
TOR1(config-if)#switchport	Configure interface as switchport
TOR1(config-if)#exit	Exit the interface mode
TOR1(config)#interface xe2	Enter interface mode
TOR1(config-if)#channel-group 3 mode active	Make part of channel group 3
TOR1(config-if)#exit	Exit the interface mode
TOR1(config)#interface xe3	Enter interface mode
TOR1(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system
TOR1(config-if)#exit	Exit the interface mode
TOR1(config-if)#interface xe49/1	Enter interface mode
TOR1(config-if)#channel-group 2 mode active	Enable channel-group 2
TOR1(config-if)#exit	Exit the interface mode
TOR1(config)#mcec domain configuration	Enter MCEC mode
TOR1(config-mcec-domain)#domain-address 2222.3333.4444	Domain address for the MLAG domain
TOR1(config-mcec-domain)#domain-system-number 1	Number to identify the node in a domain
TOR1(config-mcec-domain)#intra-domain-link po3	Intra domain line between MLAG domain

TOR1(config)#hardware-profile filter ingress-arp enable	Enable globally hardware profile for ARP
TOR1(config)#arp access-list cep	Create access list with name as CEP
TOR1(config-arp-acl)#30 permit request ip any mac host 0000.2A6C.668D vlan 3990 inner-vlan 2	Create permit rule for particular ARP request
TOR1(config-arp-acl)#40 permit response ip any any mac host 0000.2A6C.668D host 0000.2A6C.7202 vlan 3990 inner-vlan 2	Create permit rule for particular ARP response
TOR1(config)#arp access-list pnp	Create access list with name as PNP
TOR1(config-arp-acl)#20 permit request ip any mac host 0000.2A6C.7202 vlan 3990 inner-vlan 2	Create permit rule for particular ARP request
TOR1(config-arp-acl)#30 permit response ip any any mac host 0000.2A6C.7202 host 0000.2A6C.668D vlan 3990 inner-vlan 2	Create permit rule for particular ARP response
TOR1(config-if)#interface mlag1	Enter mlag1 interface
TOR1(config-if)#arp access-group cep in	Attach rule with access-group CEP
TOR1(config-if)#interface mlag2	Enter mlag2 interface
TOR1(config-if)#arp access-group pnp in	Attach rule with access-group PNP

TOR2

#configure terminal	Enter configure mode.
TOR2(config)#bridge 1 protocol provider-rstp edge	Create provider RSTP bridge
TOR2(config)#vlan 2-3990 type customer bridge 1 state enable	Enable customer VLAN for bridge
TOR2(config)#vlan 2-3990 type service point-point bridge 1 state enable	Enable service VLAN for bridge
TOR2(config)#cvlan registration table map1 bridge 1	Create registration table
TOR2(config-cvlan-registration)#cvlan 2-3990 svlan 3990	Map CVLAN to svlan
TOR2(config-cvlan-registration)#exit	Exit the CVLAN registration table mode
TOR2(config)#interface mlag1	Enter MLAG interface
TOR2(config-if)#switchport	Configure interface as switchport
TOR2(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
TOR2(config-if)#switchport mode customer-edge hybrid	Set the switching characteristics of this interface to customer-edge hybrid
TOR2(config-if)#switchport customer-edge hybrid allowed vlan all	Set the switching characteristics of this interface to customer-edge hybrid and allow VLAN all
TOR2(config-if)#switchport customer-edge vlan registration map1	Configure the registration table mapping on MLAG interface
TOR2(config-if)#exit	Exit the interface mode
TOR2(config)#interface mlag2	Enter MLAG interface

TOR2(config-if)#switchport	Configure interface as switchport
TOR2(config-if)#bridge-group 1	Associate the interface with bridge group 1
TOR2(config-if)#switchport mode provider-network	Set the switching characteristics of this interface to provider network
TOR2(config-if)#switchport provider-network allowed vlan all	Set the switching characteristics of this interface to provider network and allow all VLAN
TOR2(config-if)#exit	Exit the interface mode
TOR2(config)#interface po1	Enter dynamic LAG interface
TOR2(config-if)#switchport	Configure interface as switchport
TOR2(config-if)#mlag 1	Enable MLAG group number
TOR2(config-if)#exit	Exit the interface mode
TOR2(config)#interface po2	Enter dynamic LAG interface
TOR2(config-if)#switchport	Configure interface as switchport
TOR2(config-if)#mlag 2	Enable MLAG group number
TOR2(config-if)#exit	Exit the interface mode
TOR2(config)#interface po3	Enter dynamic LAG interface
TOR2(config-if)#switchport	Configure interface as switchport
TOR2(config-if)#exit	Exit the interface mode
TOR2(config)#interface xe2	Enter interface mode
TOR2(config-if)#channel-group 3 mode active	Make part of channel group 3
TOR2(config-if)#interface xe3	Enter interface mode
TOR2(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system
TOR2(config-if)#exit	Exit the interface mode
TOR2(config)#Interface xe49/1	Enter interface mode
TOR2(config-if)#channel-group 2 mode active	Enable channel-group 2
TOR2(config)#mcec domain configuration	Configure MCEC domain information
TOR2(config-mcec-domain)#domain-address 2222.3333.4444	Domain address for the MLAG domain
TOR2(config-mcec-domain)#domain-system-number 2	Number to identify the node in a domain
TOR2(config-mcec-domain)#intra-domain-link po3	Intra domain line between MLAG domain
TOR2(config)#hardware-profile filter ingress-arp enable	Enable globally hardware profile for ARP
TOR2(config)#arp access-list cep	Create access list with name as CEP
TOR2(config-arp-acl)#30 permit request ip any mac host 0000.2A6C.668D vlan 3990 inner-vlan 2	Create permit rule for particular ARP request
TOR2(config-arp-acl)#40 permit response ip any any mac host 0000.2A6C.668D host 0000.2A6C.7202 vlan 3990 inner-vlan 2	Create permit rule for particular ARP response
TOR2(config)#arp access-list pnp	Create access list with name as PNP

TOR2(config-arp-acl)#20 permit request ip any mac host 0000.2A6C.7202 vlan 3990 inner-vlan 2	Create permit rule for particular ARP request
TOR2(config-arp-acl)#30 permit response ip any any mac host 0000.2A6C.7202 host 0000.2A6C.668D vlan 3990 inner-vlan 2	Create permit rule for particular ARP response
TOR2(config-if)#interface mlag1	Enter mlag1 interface
TOR2(config-if)#arp access-group cep in	Attach rule with access-group CEP
TOR2(config-if)#interface mlag2	Enter mlag2 interface
TOR2(config-if)#arp access-group pnp in	Attach rule with access-group PNP

SW1

#configure terminal	Enter configure mode.
SW1(config)#bridge 1 protocol rstp vlan-bridge	Configure the RSTP VLAN bridge
SW1(config)#vlan 2-3990 type customer bridge 1 state enable	Enable customer VLAN for bridge
SW1(config-if)#interface po1	Enter dynamic LAG interface
SW1(config-if)#switchport	Configure interface as switchport
SW1(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
SW1(config-if)#switchport mode hybrid	Set the switching characteristics of this interface hybrid
SW1(config-if)#switchport hybrid allowed vlan all	Set the switching characteristics of this interface hybrid and allowing all VLAN
SW1(config-if)#exit	Exit the interface mode
SW1(config)#interface xe1	Enter interface mode
SW1(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
SW1(config-if)#exit	Exit the interface mode
SW1(config)#interface xe2	Enter interface mode
SW1(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
SW1(config-if)#exit	Exit the interface mode
SW1(config)#interface xe3	Enter interface mode
SW1(config-if)#switchport	Configure interface as switchport
SW1(config-if)#bridge-group 1 spanning-tree disable	Associate the interface with bridge group 1and disabling spanning-tree
SW1(config-if)#switchport mode hybrid	Set the switching characteristics of this interface hybrid
SW1(config-if)#switchport hybrid allowed vlan all	Set the switching characteristics of this interface hybrid and allowing all VLAN
SW1(config-if)#exit	Exit the interface mode

LEAF

`#configure terminal`	Enter configure mode.
`Leaf(config)#bridge 1 protocol provider-rstp edge`	Configure the RSTP VLAN bridge
`Leaf(config)#vlan 2-3990 type customer bridge 1 state enable`	Enable customer VLAN for bridge
`Leaf(config)#vlan 2-3990 type service point-point bridge 1 state enable`	Enable service VLAN for bridge
`Leaf(config)#cvlan registration table map1 bridge 1`	Create registration table
`Leaf(config-cvlan-registration)#cvlan 2-3990 svlan 3990`	Map CVLAN to SVLAN
`Leaf(config-if)#exit`	Exit the CVLAN registration table mode
`Leaf(config)#interface po2`	Enter interface mode
`Leaf(config-if)#switchport`	Configure interface as switchport
`Leaf(config-if)#bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1and disabling spanning-tree
`Leaf(config-if)#switchport mode provider-network`	Set the switching characteristics of this interface provider network
`Leaf(config-if)#switchport provider-network allowed vlan all`	Set the switching characteristics of this interface provider and allowing all VLAN
`Leaf(config-if)#exit`	Exit the interface mode
`Leaf(config)#interface xe1`	Enter interface mode
`Leaf(config-if)#channel-group 2 mode active`	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
`Leaf(config-if)#exit`	Exit the interface mode
`Leaf(config)#interface xe2`	Enter interface mode
`Leaf(config-if)#channel-group 2 mode active`	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
`Leaf(config-if)#exit`	Exit the interface mode
`Leaf(config)#Interface xe3`	Enter interface mode
`Leaf(config-if)#switchport`	Configure interface as switchport
`Leaf(config-if)#bridge-group 1 spanning-tree disable`	Associate the interface with bridge group 1and disabling spanning-tree
`Leaf(config-if)#switchport mode customer-edge hybrid`	Set the switching characteristics of this interface to customer-edge hybrid
`Leaf(config-if)#switchport customer-edge hybrid allowed vlan all`	Set the switching characteristics of this interface to customer-edge hybrid and allow vlan all
`Leaf(config-if)#switchport customer-edge vlan registration map1`	Configure the registration table mapping on mlag interface
`Leaf(config-if)#exit`	Exit the interface mode

Validation

```
TOR1#show access-lists
```

```
ARP access list cep
        30 permit request ip any mac host 0000.2A6C.668D vlan 3990 inner-vlan 2
        40 permit response ip any any mac host 0000.2A6C.668D host 0000.2A6C.7202 vlan
3990 inner-vlan 2
        default deny-all ARP access list pnp
        20 permit request ip any mac host 0000.2A6C.7202 vlan 3990 inner-vlan 2
[match=1]
        30 permit response ip any any mac host 0000.2A6C.7202 host 0000.2A6C.668D vlan
3990 inner-vlan 2 [match=1]
        default deny-all log

TOR2#show access-lists
ARP access list cep
        30 permit request ip any mac host 0000.2A6C.668D vlan 3990 inner-vlan 2
[match=1]
        40 permit response ip any any mac host 0000.2A6C.668D host 0000.2A6C.7202 vlan
3990 inner-vlan 2 [match=1]
        default deny-all log ARP access list pnp
        20 permit request ip any mac host 0000.2A6C.7202 vlan 3990 inner-vlan 2
        30 permit response ip any any mac host 0000.2A6C.7202 host 0000.2A6C.668D vlan
3990 inner-vlan 2
        default deny-all
```

CHAPTER 15 PW Redundancy with MLAG Configuration

This chapter contains configuration for Pseudowire Redundancy with MLAG (Active and Standby). It also provides an overview of Pseudowire concepts.

In a single-segment pseudowire (SS-PW) application, the Packet Switched Network (PSN) layer usually provides protection for the PW. One way is by using an RSVP LSP with Fast Reroute (FRR) backup; another way is an end-to-end backup LSP. However, there are some applications where the backup PW terminates on a different target PE node, so PSN protection methods cannot protect against failure of either the target Provider Edge (PE) node or a remote Access Circuit (AC). It is also important for an operator that a particular PW is preferred. For example, the one with the least latency.

PW redundancy supports Label Distribution Protocol (LDP) PW. In the case of PW applications, the PSN layer can provide the protection for PW. Occasionally, a TE LSP signaled by RSVP-TE can be used as a PSN tunnel for a PW. In this scenario, TE can provide FRR to protect the end-to-end LSP in the PSN layer.

FRR-based protection schemes cannot protect against failure of PE nodes and access circuits. However, PW redundancy can protect against these failures.

MLAG expands the concept of link aggregation so that it provides node-level redundancy by allowing two nodes to share a common LAG endpoint. This gives PE redundancy for CE node.

CE devices can be connected to two PE nodes for PE-node-level redundancy using MLAG.

End-to-End traffic flow decision will take by MLAG Active node not by PW-Redundancy node.

Topology

In the below example PE1 and PE2 forms a MLAG domain.

As shown in Figure 15-35, PE1 and PE2 are a single logical switches to P3 and P4. Even if either PE1 or PE2 is down, there exists a path to reach other destinations.

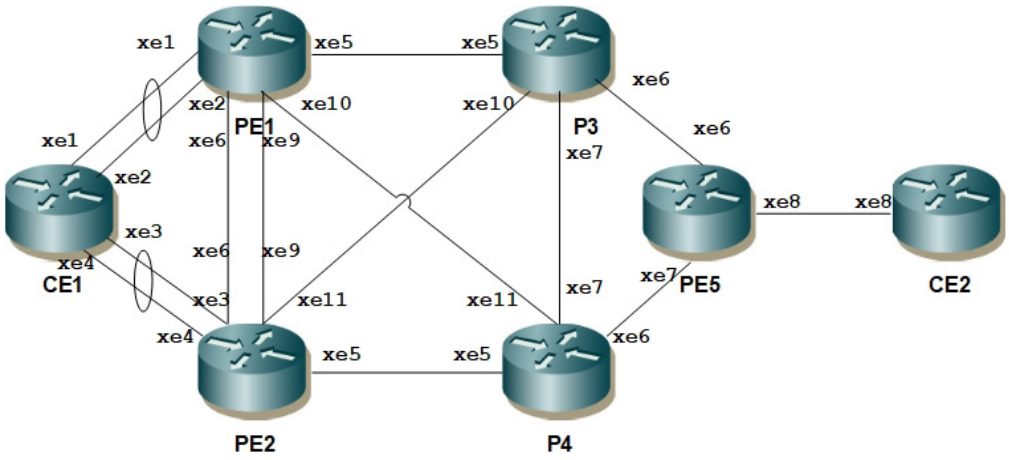


Figure 15-35: MLAG Topology

Uplink Interface and OSPF Configuration

PE1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Configure the Loopback interface.
`(config-if)# ip address 35.35.35.35/32 secondary`	Set the IP address of the loopback interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe5`	Enter interface mode.
`(config-if)# ip address 10.35.48.1/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe9`	Enter interface mode.
`(config-if)# ip address 10.35.33.1/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe10`	Enter interface mode.
`(config-if)# ip address 10.35.49.1/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Enter the Router mode for OSPF.
`(config-router)#ospf router-id 35.35.35.35`	Configure OSPF router ID.
`(config-router)# bfd all-interfaces`	Configure BFD on OSPF.
`(config-router)#network 10.35.48.0/30 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`(config-router)#network 10.35.49.0/30 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`(config-router)#network 10.35.33.0/30 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`(config-router)#exit`	Exit router mode.

PE2

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Configure the Loopback interface.
`(config-if)# ip address 33.33.33.33/32 secondary`	Set the IP address of the loopback interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe5`	Enter interface mode.
`(config-if)# ip address 10.33.49.1/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe9`	Enter interface mode.
`(config-if)# ip address 10.35.33.2/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe11`	Enter interface mode.

(config-if)# ip address 10.33.48.1/30	Set the IP address of the interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf 100	Enter the Router mode for OSPF.
(config-router)#ospf router-id 33.33.33.33	Configure OSPF router ID.
(config-router)# bfd all-interfaces	Configure BFD on OSPF.
(config-router)#network 10.33.48.0/30 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
(config-router)#network 10.33.49.0/30 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
(config-router)#network 10.35.33.0/30 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
(config-router)#exit	Exit router mode

P3

#configure terminal	Enter configure mode.
(config)#interface lo	Configure the Loopback interface.
(config-if)# ip address 48.48.48.48/32 secondary	Set the IP address of the loopback interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe5	Enter interface mode.
(config-if)# ip address 10.35.48.2/30	Set the IP address of the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe6	Enter interface mode.
(config-if)# ip address 10.48.32.1/30	Set the IP address of the interface
(config-if)#exit	Exit interface mode.
(config)# interface xe7	Enter interface mode.
(config-if)# ip address 10.48.49.1/30	Set the IP address of the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe11	Enter interface mode.
(config-if)# ip address 10.33.48.2/30	Set the IP address of the interface
(config-if)#exit	Exit interface mode.
(config)#router ospf 100	Enter the Router mode for OSPF.
(config-router)#ospf router-id 48.48.48.48	Configure OSPF router ID.
(config-router)# bfd all-interfaces	Configure BFD on OSPF.
(config-router)#network 10.35.48.0/30 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
(config-router)#network 10.48.49.0/30 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
(config-router)#network 10.48.32.0/30 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
(config-router)#network 10.33.48.0/30 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
(config-router)#exit	Exit router mode

P4

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Configure the Loopback interface.
`(config-if)# ip address 49.49.49.49/32 secondary`	Set the IP address of the loopback interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe5`	Enter interface mode.
`(config-if)# ip address 10.33.49.2/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe6`	Enter interface mode.
`(config-if)# ip address 10.49.32.1/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe7`	Enter interface mode.
`(config-if)# ip address 10.48.49.2/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe10`	Enter interface mode.
`(config-if)# ip address 10.35.49.2/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Enter the Router mode for OSPF.
`(config-router)#ospf router-id 49.49.49.49`	Configure OSPF router ID.
`(config-router)# bfd all-interfaces`	Configure BFD on OSPF.
`(config-router)#network 10.35.49.0/30 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`(config-router)#network 10.48.49.0/30 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`(config-router)#network 10.49.32.0/30 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`(config-router)#network 10.33.49.0/30 area 0.0.0.0`	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
`(config-if)#exit`	Exit interface mode.

P5

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Configure the Loopback interface.
`(config-if)# ip address 32.32.32.32/32 secondary`	Set the IP address of the loopback interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe6`	Enter interface mode.
`(config-if)# ip address 10.48.32.2/30`	Set the IP address of the interface.
`(config-if)#exit`	Exit interface mode.

(config)# interface xe7	Enter interface mode.
(config-if)# ip address 10.49.32.1/30	Set the IP address of the interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf 100	Enter the Router mode for OSPF.
(config-router)#ospf router-id 32.32.32.32	Configure OSPF router ID.
(config-router)# bfd all-interfaces	Configure BFD on OSPF.
(config-router)#network 10.48.32.0/30 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
(config-router)#network 10.49.32.0/30 area 0.0.0.0	Define the Network on which OSPF runs and associate the area ID (area 0) with the interface.
(config-if)#exit	Exit interface mode.

RSVP Global Configuration

PE1

#configure terminal	Enter configure mode.
(config)#router rsvp	Enter the router mode for RSVP.
(config-router)# no php	Configure no PHP
(config-router)#exit	Exit router mode.
(config)# interface xe5	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe9	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe10	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.

PE2

#configure terminal	Enter configure mode.
(config)#router rsvp	Enter the Router mode for RSVP.
(config-router)# no php	Configure no PHP
(config-router)#exit	Exit router mode.
(config)# interface xe5	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface

(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe9	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface.
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe11	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.

P3

#configure terminal	Enter configure mode.
(config)#router rsvp	Enter the Router mode for RSVP.
(config-router)# no php	Configure no PHP
(config-router)#exit	Exit router mode.
(config)# interface xe5	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe6	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe7	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe11	Enter interface mode.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.

P4

#configure terminal	Enter configure mode.
(config)#router rsvp	Enter the Router mode for RSVP.
(config-router)# no php	Configure no PHP
(config-router)#exit	Exit router mode.

`(config)# interface xe5`	Enter interface mode.
`(config-if)# label-switching`	Enable label switching on the interface
`(config-if)# enable-rsvp`	Enable RSVP on the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe6`	Enter interface mode.
`(config-if)# label-switching`	Enable label switching on the interface
`(config-if)# enable-rsvp`	Enable RSVP on the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe7`	Enter interface mode.
`(config-if)# label-switching`	Enable label switching on the interface
`(config-if)# enable-rsvp`	Enable RSVP on the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe10`	Enter interface mode.
`(config-if)# label-switching`	Enable label switching on the interface
`(config-if)# enable-rsvp`	Enable RSVP on the interface.
`(config-if)#exit`	Exit interface mode.

P5

`#configure terminal`	Enter configure mode.
`(config)#router rsvp`	Enter the Router mode for RSVP.
`(config-router)# no php`	Configure no PHP
`(config-router)#exit`	Exit router mode.
`(config)# interface xe6`	Enter interface mode.
`(config-if)# label-switching`	Enable label switching on the interface
`(config-if)# enable-rsvp`	Enable RSVP on the interface.
`(config-if)#exit`	Exit interface mode.
`(config)# interface xe7`	Enter interface mode.
`(config-if)# label-switching`	Enable label switching on the interface
`(config-if)# enable-rsvp`	Enable RSVP on the interface.
`(config-if)#exit`	Exit interface mode.

RSVP-LSP Configuration

PE1

`#configure terminal`	Enter configure mode.
`(config)# rsvp-path 35-to-32 mpls`	Configure RSVP-Path PE5
`(config-path)# 10.35.48.2 strict`	Configure Strict hop

(config-path)# 10.48.32.2 strict	Configure Strict hop
(config-path)#exit	Exit RSVP-Path mode
(config)#rsvp-trunk 35-to-32	Configure RSVP-Trunk to PE5
(config-trunk)# primary fast-reroute protection one-to-one	Set FRR one-to-one mode.
(config-trunk)# primary fast-reroute node-protection	Set FRR node protection
(config-trunk)# primary path 35-to-32	Set RSVP path.
(config-trunk)# to 32.32.32.32	Configure RSVP-LSP destination IP address
(config-trunk)#exit	Exit RSVP-Trunk mode

PE2

#configure terminal	Enter configure mode.
(config)# rsvp-path 33-to-32 mpls	Configure RSVP-Path to PE5
(config-path)# 10.33.49.2 strict	Configure Strict hop
(config-path)# 10.49.32.2 strict	Configure Strict hop
(config-path)#exit	Exit RSVP path mode
(config)#rsvp-trunk 33-to-32	Configure RSVP trunk to PE5.
(config-trunk)# primary fast-reroute protection one-to-one	Set FRR one-to-one mode.
(config-trunk)# primary fast-reroute node-protection	Set FRR node protection
(config-trunk)# primary path 33-to-32	Set RSVP path.
(config-trunk)# to 32.32.32.32	Configure RSVP LSP destination IP address.
(config-trunk)#exit	Exit RSVP-Trunk mode

PE5

#configure terminal	Enter configure mode.
(config)# rsvp-path 32-to-35 mpls	Configure RSVP path to PE1
(config-path)# 10.48.32.1 strict	Configure Strict hop
(config-path)# 10.35.48.1 strict	Configure Strict hop
(config-path)#exit	Exit RSVP path mode
(config)# rsvp-path 32-to-33 mpls	Configure RSVP path to PE2
(config-path)# 10.49.32.1 strict	Configure Strict hop
(config-path)# 10.33.49.1 strict	Configure Strict hop
(config-path)#exit	Exit RSVP path mode
(config)#rsvp-trunk 32-to-35	Configure RSVP trunk.to PE1.
(config-trunk)# primary fast-reroute protection one-to-one	Set FRR one-to-one mode.
(config-trunk)# primary fast-reroute node-protection	Set FRR node protection

(config-trunk)# primary path 32-to-35	Set RSVP path
(config-trunk)# to 33.33.33.33	Configure RSVP-LSP destination IP address.
(config-trunk)#exit	Exit RSVP trunk mode

T-LDP Configuration

PE1

#configure terminal	Enter configure mode.
(config)#router ldp	Enter the router mode for LDP.
(config-router)# router-id 35.35.35.35	Configure LDP router ID.
(config-router)# pw-status-tlv	Set PW status TLV
(config-router)# no multicast-hellos	Disable Multicast hellos
(config-router)# targeted-peer ipv4 32.32.32.32	Configure LDP targeted peer to PE5
(config-router-targeted-peer)# exit-targeted-peer-mode	Exit targeted peer mode.
(config-router)#exit	Exit router mode
(config)# interface xe5	Enter interface mode.
(config-if)# enable-ldp ipv4	Enable IPv4 LDP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe9	Enter interface mode.
(config-if)# enable-ldp ipv4	Enable IPv4 LDP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe10	Enter interface mode.
(config-if)# enable-ldp ipv4	Enable IPv4 LDP on the interface.
(config-if)#exit	Exit interface mode.

PE2

#configure terminal	Enter configure mode.
(config)#router ldp	Enter the router mode for LDP.
(config-router)# router-id 33.33.33.33	Configure LDP router ID
(config-router)# pw-status-tlv	Set PW status TLV.
(config-router)# no multicast-hellos	Disable multicast hellos
(config-router)# targeted-peer ipv4 32.32.32.32	Configure LDP targeted peer to PE5
(config-router-targeted-peer)# exit-targeted-peer-mode	Exit targeted peer mode.
(config-router)#exit	Exit router mode
(config)# interface xe5	Enter interface mode.

(config-if)# enable-ldp ipv4	Enable IPv4 LDP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe9	Enter interface mode.
(config-if)# enable-ldp ipv4	Enable IPv4 LDP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe11	Enter interface mode.
(config-if)# enable-ldp ipv4	Enable IPv4 LDP on the interface.
(config-if)#exit	Exit interface mode.

PE5

#configure terminal	Enter configure mode.
(config)#router ldp	Enter the router mode for LDP.
(config-router)# router-id 32.32.32.32	Configure LDP router ID
(config-router)# pw-status-tlv	Set PW status TLV
(config-router)# no multicast-hellos	Disable multicast hellos
(config-router)# targeted-peer ipv4	Configure LDP targeted peer to PE5
(config-router-targeted-peer)# exit-targeted-peer-mode	Exit targeted peer mode.
(config-router)# targeted-peer ipv4 33.33.33.33	Configure LDP targeted peer to PE5
(config-router-targeted-peer)# exit-targeted-peer-mode	Exit targeted peer mode.
(config-router)#exit	Exit router mode
(config)# interface xe6	Enter interface mode.
(config-if)# enable-ldp ipv4	Enable IPv4 LDP on the interface.
(config-if)#exit	Exit interface mode.
(config)# interface xe7	Enter interface mode.
(config-if)# enable-ldp ipv4	Enable IPv4 LDP on the interface.
(config-if)#exit	Exit interface mode.

MLAG Configuration

CE1

#configure terminal	Enter configure mode.
(config)#interface po1	Configure the LAG interface
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode.

(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by
(config-if)#exit	Exit interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by
(config-if)#exit	Exit interface mode.
(config)#interface xe4	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by
(config-if)#exit	Exit interface mode.

PE1

#configure terminal	Enter configure mode.
(config)#mcec domain configuration	Configure MLAG global.
(config-mcec-domain)# domain-address 1111.2222.3333	Configure the domain address.
(config-mcec-domain)# domain-system-number 1	Configure Domain System number.
(config-mcec-domain)# intra-domain-link xe6	Configure IDL link.
(config-mcec-domain)#exit	Exit MLAG global mode.
(config)#interface po1	Configure the LAG interface
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by
(config-if)#exit	Exit interface mode.
(config)#interface po1	Configure the LAG interface
(config-if)# mlag 1	Configure MLAG domain to LAG interface
(config-if)#exit	Exit interface mode.

PE2

`#configure terminal`	Enter configure mode.
`(config)#mcec domain configuration`	Configure MLAG global
`(config-mcec-domain)# domain-address 1111.2222.3333`	Configure the Domain address
`(config-mcec-domain)# domain-system-number 2`	Configure Domain System number.
`(config-mcec-domain)# intra-domain-link xe6`	Configure IDL link.
`(config-mcec-domain)#exit`	Exit MLAG global mode.
`(config)#interface po1`	Configure the LAG interface
`(config-if)#switchport`	Configure the interface as Layer 2
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe3`	Enter interface mode.
`(config-if)#channel-group 1 mode active`	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe4`	Enter interface mode.
`(config-if)#channel-group 1 mode active`	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by
`(config-if)#exit`	Exit interface mode.
`(config)#interface po1`	Configure the LAG interface
`(config-if)# mlag 1`	Configure MLAG domain to LAG interface
`(config-if)#exit`	Exit interface mode.

VPWS PW Redundancy Configuration

PE1

`#configure terminal`	Enter configure mode.
`(config)#service-template S-00-00-10`	Configure service template (translate)
`(config-svc)# match outer-vlan 10`	Configure match
`(config-svc)# rewrite ingress translate 20 outgoing-tpid dot1.q`	Configure rewrite action
`(config-svc)#exit`	Exit service template
`(config)# mpls l2-circuit VC1 1001 32.32.32.32`	Configure VPWS to PE5
`(config-pseudowire)#exit`	Exit pseudowire config mode.
`(config)#int po1`	Enter interface mode
`(config-if)#mpls-l2-circuit VC1 service-template S-00-00-10`	Attach VPWS to AC interface.
`(config-if)#exit`	Exit interface

PE2

`#configure terminal`	Enter configure mode.
`(config)#service-template S-00-00-10`	Configure service template (translate)
`(config-svc)# match outer-vlan 10`	Configure match
`(config-svc)# rewrite ingress translate 20 outgoing-tpid dot1.q`	Configure rewrite action
`(config-svc)#exit`	Exit service template
`(config)# mpls l2-circuit VC2 1002 32.32.32.32`	Configure VPWS to PE5
`(config-pseudowire)#exit`	Exit pseudowire config mode.
`(config)#int po1`	Enter interface mode
`(config-if)#mpls-l2-circuit VC2 service-template S-00-00-10`	Attach VPWS to AC interface.
`(config-if)#exit`	Exit interface

PE5

`#configure terminal`	Enter configure mode.
`(config)#service-template S-00-00-10`	Configure service template (translate)
`(config-svc)# match outer-vlan 10`	Configure match
`(config-svc)# rewrite ingress translate 20 outgoing-tpid dot1.q`	Configure rewrite action
`(config-svc)#exit`	Exit service template
`(config)# mpls l2-circuit VC1 1001`	Configure VPWS to PE1
`(config-pseudowire)#exit`	Exit pseudowire config mode.
`(config)# mpls l2-circuit VC2 1002 33.33.33.33`	Configure VPWS to PE2
`(config-pseudowire)#exit`	Exit pseudowire config mode.
`(config)#int xe8`	Enter interface mode
`(config-if)# switchport`	Switch to Layer 2 mode.
`(config-if)#mpls-l2-circuit VC1 service-template S-00-00-10`	Attach Primary VPWS to AC interface.
`(config-if)# mpls-l2-circuit VC2 service-template S-00-00-10 secondary`	Attach Secondary VPWS to AC interface.
`(config-if)#exit`	Exit interface

Validation

To see detail information about the MLAG, use the following command:

MLAG Active node:

```
PE1#show mlag domain details
```

```
-----------------------------------
Domain Configuration
-----------------------------------

Domain System Number           : 1
Domain Address                 : 1111.2222.3333
Domain Priority                : 32768
Intra Domain Interface         : xe12

Hello RCV State                : Current
Hello Periodic Timer State     : Slow Periodic
Domain Sync                    : IN_SYNC
Neigh Domain Sync              : IN_SYNC
Domain Adjacency               : UP

-----------------------------------
MLAG Configuration
-----------------------------------

MLAG-1
  Mapped Aggregator            : po1
  Admin Key                    : 16385
  Oper Key                     : 16385
  Physical properties Digest   : 89 25 47 22 f1 47 6d 92 b8 71 9c ca 61 fb db
3a

  Neigh Admin Key              : 32769
  Neigh Physical Digest        : 89 25 47 22 f1 47 6d 92 b8 71 9c ca 61 fb db
3a
  Info RCV State               : Current
  Info Periodic Time State     : Standby
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Standby
  Current Mlag state           : Active
```

MLAG Standby node:

```
PE2#show mlag domain details

-----------------------------------
Domain Configuration
-----------------------------------

Domain System Number           : 2
Domain Address                 : 1111.2222.3333
Domain Priority                : 32768
Intra Domain Interface         : xe12

Hello RCV State                : Current
Hello Periodic Timer State     : Slow Periodic
Domain Sync                    : IN_SYNC
Neigh Domain Sync              : IN_SYNC
Domain Adjacency               : UP

-----------------------------------
```

```
MLAG Configuration
-----------------------------------

MLAG-1
  Mapped Aggregator            : po1
  Admin Key                    : 32769
  Oper Key                     : 32769
  Physical properties Digest   : 89 25 47 22 f1 47 6d 92 b8 71 9c ca 61 fb db
3a

  Neigh Admin Key              : 16385
  Neigh Physical Digest        : 89 25 47 22 f1 47 6d 92 b8 71 9c ca 61 fb db
3a
  Info RCV State               : Current
  Info Periodic Time State     : Standby
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Standby
  Current Mlag state           : Standby
```

To see summary information about the MLAG, use the following command:

MLAG active node:

```
PE1#show mlag domain summary

-----------------------------------
Domain Configuration
-----------------------------------

Domain System Number            : 2
Domain Address                  : 1111.2222.3333
Domain Priority                 : 32768
Intra Domain Interface          : xe12
Domain Adjacency                : UP
Domain Sync via                 : Intra-domain-interface
-----------------------------------
MLAG Configuration
-----------------------------------

MLAG-1
  Mapped Aggregator            : po1
  Physical properties Digest   : 89 25 47 22 f1 47 6d 92 b8 71 9c ca 61 fb db
3a
  Total Bandwidth              : 20g
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Standby
  Current Mlag state           : Active
```

MLAG Standby node:

```
PE2#show mlag domain summary

-----------------------------------
Domain Configuration
-----------------------------------

Domain System Number            : 1
```

```
Domain Address                   : 1111.2222.3333
Domain Priority                  : 32768
Intra Domain Interface           : xe12
Domain Adjacency                 : UP
Domain Sync via                  : Intra-domain-interface
-----------------------------------
MLAG Configuration
-----------------------------------

MLAG-1
  Mapped Aggregator              : po1
  Physical properties Digest     : 89 25 47 22 f1 47 6d 92 b8 71 9c ca 61 fb db
3a
  Total Bandwidth                : 20g
  Mlag Sync                      : IN_SYNC
  Mode                           : Active-Standby
      Current Mlag state           : Standby
```

To see summary information about the Virtual Circuits, use the following command:

```
#show mpls vc-table
The samples below show summary information about the just-configured four
virtual circuits.
PE1#show mpls vc-table
VC-ID       Vlan-ID  Inner-Vlan-ID  Access-Intf   Network-Intf  Out Label
Tunnel-Label  Nexthop         Status
1001        N/A      N/A            po1           xe14          24960
24324         32.32.32.32     Active
PE1#

PE2#show mpls vc-table
VC-ID       Vlan-ID  Inner-Vlan-ID  Access-Intf   Network-Intf  Out Label
Tunnel-Label  Nexthop         Status
1002        N/A      N/A            po1           xe14          24961
24323         32.32.32.32     Inactive
PE2#

PE5#show mpls vc-table
VC-ID       Vlan-ID  Inner-Vlan-ID  Access-Intf   Network-Intf  Out Label
Tunnel-Label  Nexthop         Status
1001        N/A      N/A            xe23          xe12          24986
24322         35.35.35.35     Active
1002        N/A      N/A            xe23          xe12          24968
24320         33.33.33.33     Inactive
PE5#
```

To view detailed configuration information about the L2 Virtual Circuits, including LDP PW status, use the following command:

```
PE1#show ldp mpls-l2-circuit 1001 detail
vcid: 1001  type: vlan, local groupid: 0, remote groupid: 0 (vc is up)
destination: 32.32.32.32, Peer LDP Ident: 32.32.32.32
Local label: 24986, remote label: 24960
Access IF: po1, Network IF: xe13
Local MTU: 9100, Remote MTU: 9100
Local Control Word: disabled  Remote Control Word: Not-Applicable  Current
use: disabled
```

```
Local PW Status Capability : enabled
Remote PW Status Capability : enabled
Current PW Status TLV : enabled
Local PW Status :
  Forwarding
  Active
Remote PW Status :
  Forwarding
  Active

PE2#show ldp mpls-l2-circuit 1002 detail
vcid: 1002  type: vlan, local groupid: 0, remote groupid: 0 (vc is up)
destination: 32.32.32.32, Peer LDP Ident: 32.32.32.32
Local label: 24968, remote label: 24961
Access IF: po1, Network IF: xe14
Local MTU: 9100, Remote MTU: 9100
Local Control Word: disabled  Remote Control Word: Not-Applicable  Current
use: disabled
Local PW Status Capability : enabled
Remote PW Status Capability : enabled
Current PW Status TLV : enabled
Local PW Status :
  Not Forwarding
  Ingress AC Receive Fault
  Egress AC Transmit Fault
Remote PW Status :
  Not Forwarding
  Standby

PE5#show ldp mpls-l2-circuit 1001 detail
vcid: 1001  type: vlan, local groupid: 0, remote groupid: 0 (vc is up)
destination: 35.35.35.35, Peer LDP Ident: 35.35.35.35
Local label: 24960, remote label: 24986
Access IF: xe23, Network IF: xe14
Local MTU: 9100, Remote MTU: 9100
Local Control Word: disabled  Remote Control Word: Not-Applicable  Current
use: disabled
Local PW Status Capability : enabled
Remote PW Status Capability : enabled
Current PW Status TLV : enabled
Local PW Status :
  Forwarding
  Active
Remote PW Status :
  Forwarding
  Active

PE5#show ldp mpls-l2-circuit 1002 detail
vcid: 1002  type: vlan, local groupid: 0, remote groupid: 0 (vc is up)
destination: 33.33.33.33, Peer LDP Ident: 33.33.33.33
Local label: 24961, remote label: 24968
Access IF: xe23, Network IF: xe12
Local MTU: 9100, Remote MTU: 9100
Local Control Word: disabled  Remote Control Word: Not-Applicable  Current
use: disabled
Local PW Status Capability : enabled
Remote PW Status Capability : enabled
Current PW Status TLV : enabled
```

```
Local PW Status :
  Not Forwarding
  Standby
Remote PW Status :
  Not Forwarding
  Ingress AC Receive Fault
  Egress AC Transmit Fault
```

CHAPTER 16 Traffic Mirroring Configuration

This chapter contains a sample local and remote switched port analyzer feature configuration.

SPAN Overview

Switched Port Analyzer (SPAN) refers to selecting network traffic for analysis by a network analyzer. SPAN feature is introduced on switches as the switch forwards traffic that is destined for a MAC address directly to the corresponding port leaving no scope to analyze the traffic.

SPAN monitors the traffic on source port and sends a copy of the traffic to a destination port. The network analyzer, which is attached to the destination port, analyzes the received traffic. Source port can be a single port or multiple ports. A replication of the packets is sent to the destination port for analysis

SPAN is originally referred to port mirroring or port monitoring where all the network traffic on the source port is mirrored to destination port. Port mirroring has three subdivisions.

- Ingress mirroring: Traffic received on the source port will be monitored
- Egress mirroring: Traffic transmitted from the source port will be monitored
- Ingress and egress mirroring: Both received and transmitted traffic on the source port will be monitored.

With enhancements to SPAN, mirroring can be classified into three categories.

Port Mirroring

In port mirroring, source will be a port which could be a physical interface or a port channel. All the traffic on the source port will be mirrored to destination port. Either traffic received on the source port or traffic transmitted from the source port or both can be monitored.

Note:

- The TPID for mirrored traffic is set to 0x8100 only when the egress packet is mirrored.
- When ingress traffic is mirrored, the TPID is maintained as 0x88a8.

VLAN Mirroring

In VLAN mirroring, the source is a VLAN identifier and the traffic received on all ports with the VLAN identifier matching source VLAN identifier are mirrored to destination port.

Rule Based Mirroring

In rule based mirroring, there is a set of matching criteria for the ingress traffic such as matching destination MAC address, matching frame type, and so on. The traffic matching the rules is mirrored to the destination port

Topology

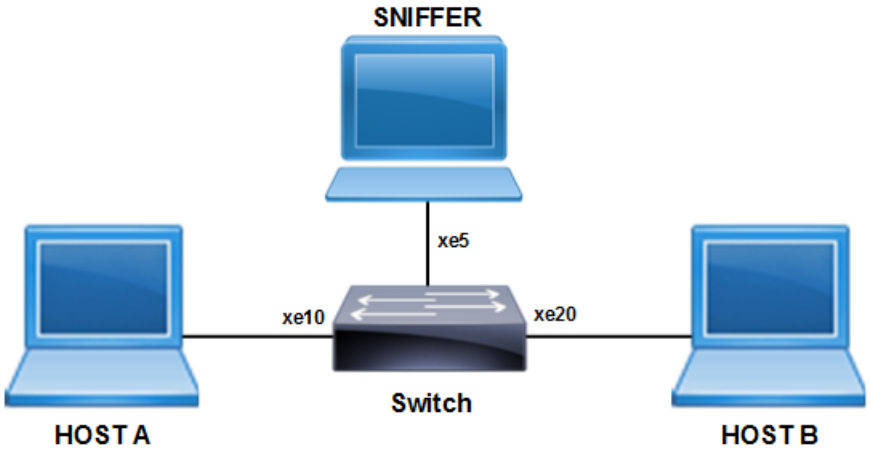


Figure 16-36: SPAN Topology

Port Mirroring Configuration

This example shows detailed configuration of port mirroring.

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)# vlan 101-110 bridge 1 state enable`	Configure VLANs.
`(config)#interface xe10`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe20`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe5`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)#exit`	Exit interface mode.

`(config)# monitor session 1`	Enter monitor session configuration mode
`(config-monitor)# destination interface xe5`	Configure the interface as destination port
`(config-monitor)# source interface xe10 both`	Configure the source interface to mirror ingress as well as egress direction traffic
`(config-monitor)# no shut`	Activate monitor session
`(config-monitor)#end`	Exit monitor session configuration mode

Validation

Enter the below commands to confirm the configurations.

```
#show running-config monitor
!
monitor session 1
 source interface xe10 both
 destination interface xe5
 no shut

#show monitor session all
   session 1
---------------
type              : local
state             : up
source intf       :
    tx            : xe10
    rx            : xe10
    both          : xe10
source VLANs      :
    rx            :
destination ports : xe5
filter count      :

Legend: f = forwarding enabled, l = learning enabled
```

VLAN and Rule Based Mirroring

This example shows detailed configuration of VLAN with rule based mirroring.

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)# vlan 101-110 bridge 1 state enable`	Configure VLANs
`(config)#interface xe10`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe20`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe5`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)#exit`	Exit interface mode.
`(config)# monitor session 1`	Enter monitor session configuration mode
`(config-monitor)# destination interface xe5`	Configure the interface as destination port
`(config-monitor)# source vlan 101`	Configure source VLAN to be mirrored
`(config-monitor)# filter src-mac host 0000.0000.0005`	Configure the rule to match the source MAC
`(config-monitor)# no shut`	Activate monitor session
`(config-monitor)#end`	Exit monitor session configuration mode

Validation

Enter the below commands to confirm the configurations.

```
#show running-config monitor
!
monitor session 1
 source vlan 101
 destination interface xe5
```

```
 10 filter src-mac host 0000.0000.0005
 no shut


#show monitor session all
   session 1
---------------
type              : local
state             : up
source intf       :
    tx            :
    rx            :
    both          :
source VLANs      :
    rx            : 101
destination ports : xe5
filter count      : 1

Legend: f = forwarding enabled, l = learning enabled


#show monitor session 1 filter
   session 1
---------------
filter count      : 1

  ---------------
  match set 1
  ---------------
  source mac address : 0000.0000.0005 (host)
```

RSPAN Overview

When several switches need to be analyzed with a single centralized sniffer, remote switched port analyzer (RSPAN) is used. In RSPAN, all the mirrored traffic will be tagged with a RSPAN VLAN ID and forwarded to remote destination via a port called reflector port. Reflector port will have the same characteristics of a local destination port. RSPAN VLAN ID will be a dedicated VLAN for the monitoring purpose and will not participate in bridging. RSPAN destination switch will strip the RSPAN VLAN tag and send it the sniffer for analysis. RSPAN will have the same sub-categories as SPAN except that the mirrored traffic will be tagged with RSPAN VLAN header and forwarded to destination switch for analysis.

Topology

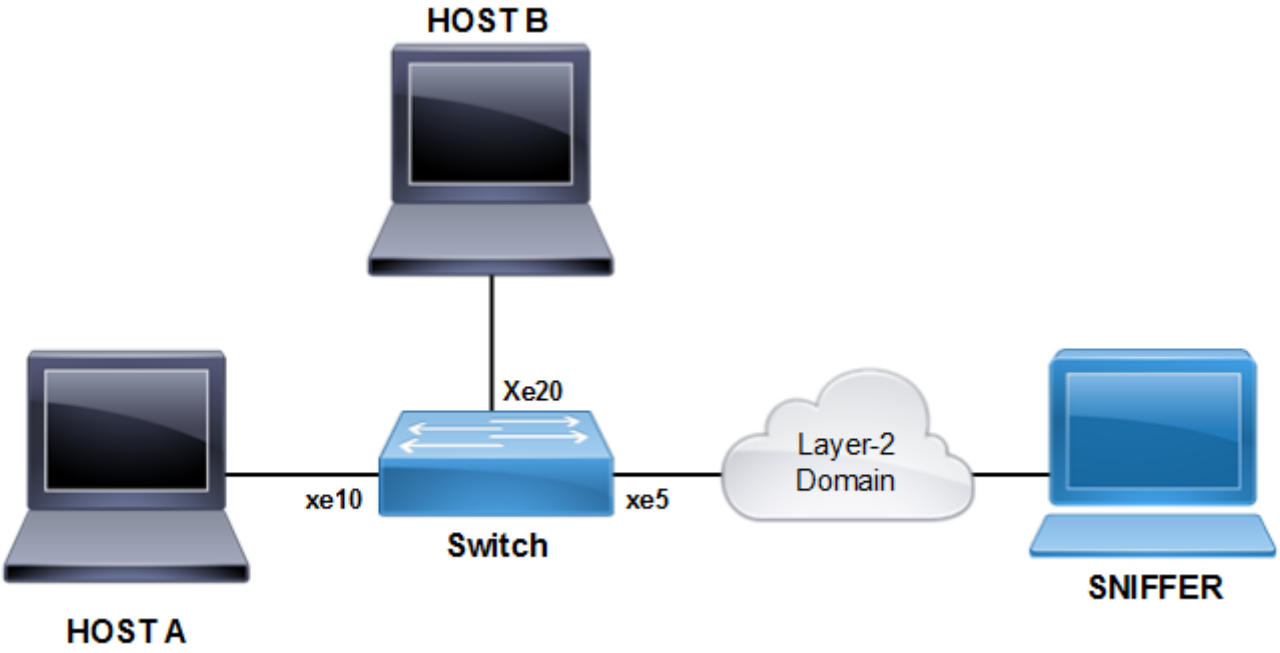


Figure 16-37: RSPAN Topology

Port Mirroring Configuration

This example shows detailed configuration of port mirroring.

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)# vlan 101-110 bridge 1 state enable`	Configure VLANs.
`(config)#interface xe10`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.

(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up.
(config-if)#exit	Exit interface mode.
(config)#interface xe20	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)# bridge-group 1	Associate bridge to an interface.
(config-if)# switchport mode trunk	Configure port as a trunk.
(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up.
(config-if)#exit	Exit interface mode.
(config)#interface xe5	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)#exit	Exit interface mode.
(config)# monitor session 1 type remote	Enter monitor session configuration mode.
(config-monitor)# destination remote vlan 100 reflector-port xe5	Configure the interface as remote destination port
(config-monitor)# source interface xe10 both	Configure the source interface to mirror ingress as well as egress direction traffic.
(config-monitor)# no shut	Activate monitor session.
(config-monitor)#end	Exit monitor session configuration mode.

Validation

Enter the commands below to confirm the configurations

```
#show running-config monitor
!
monitor session 1 type remote
 source interface xe10 both
 destination remote vlan 100 reflector-port xe5
 no shut


#show monitor session all
   session 1
---------------
type               : remote
state              : up
source intf        :
    tx             : xe10
    rx             : xe10
    both           : xe10
source VLANs       :
    rx             :
rspan VLAN         : 100
```

```
reflector ports   : xe5
filter count      :

Legend: f = forwarding enabled, l = learning enabled
```

VLAN and Rule Based Mirroring Configuration

This example shows detailed configuration of VLAN with rule based mirroring.

#configure terminal	Enter configure mode.
(config)# bridge 1 protocol mstp	Configure bridge 1 as MSTP bridge.
(config)# vlan 101-110 bridge 1 state enable	Configure VLANs.
(config)#interface xe10	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)# bridge-group 1	Associate bridge to an interface.
(config-if)# switchport mode trunk	Configure port as a trunk.
(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up.
(config-if)#exit	Exit interface mode.
(config)#interface xe20	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)# bridge-group 1	Associate bridge to an interface.
(config-if)# switchport mode trunk	Configure port as a trunk.
(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up.
(config-if)#exit	Exit interface mode.
(config)#interface xe5	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)#exit	Exit interface mode.
(config)# monitor session 1 type remote	Enter monitor session configuration mode.
(config-monitor)# destination remote vlan 100 reflector-port xe5	Configure the interface as remote destination port.
(config-monitor)# source vlan 101	Configure source VLAN to be mirrored.
(config-monitor)# filter src-mac host 0000.0000.0005	Configure the rule to match the source MAC.
(config-monitor)# no shut	Activate monitor session.
(config-monitor)#end	Exit monitor session configuration mode.

Validation

Enter the commands below to confirm the configuration.

```
#show running-config monitor
!
monitor session 1 type remote
 source vlan 101
```

```
 destination remote vlan 100 reflector-port xe5
 10 filter src-mac host 0000.0000.0005
 no shut


#show monitor session all
   session 1
---------------
type              : remote
state             : up
source intf       :
    tx            :
    rx            :
    both          :
source VLANs      :
    rx            : 101
rspan VLAN        : 100
reflector ports   : xe5
filter count      : 1

Legend: f = forwarding enabled, l = learning enabled


#show monitor session 1 filter
   session 1
---------------
filter count      : 1

  ---------------
  match set 1
  ---------------
  source mac address : 0000.0000.0005 (host)
```

CHAPTER 17 Port Security Configuration

The Port Security feature allows network administrators to block unauthorized access to the network. Network administrators can configure each port of the switch to allow network access from only secured MACs, so that the switch forwards traffic from only secured MACs.

Users can limit each port's ingress traffic by limiting MAC addresses (source MACs) that are used to send traffic into ports. Port Security enables users to configure the maximum number of secured MACs for each port. Switches learn secured MAC dynamically (learned by switch during traffic inflow) or statically (User configured MACs). Dynamically Learned or statically programmed MAC addresses cannot exceed the maximum number of secured MACs configured for a particular port. Once the switch reaches the maximum limit for secured MACs, traffic from all other MAC addresses are dropped.

The violated MACs are logged in syslog messages. Refer to `cpu queue portsec-drop` using the command `show interface cpu counter queue-stats` for information on the number of violated MACs.

Note: When configuring port-security over MLAG, configure the port-security in both MASTER and SLAVE MLAG nodes.

Note: When a port-security limit 2X is configured on MLAG (X in Master and X in Slave), the total number of secured MACs could be less than 2X if most of the traffic is load-balanced with one MLAG node which is not capable of securing more than X MACs even if peer MLAG node has secured less than X MACs.

Secured MACs Learned Dynamically

Figure 17-38: Secured MACs learned dynamically

Send Layer 2 traffic with incremental source MAC of 100 and with VLAN 100 from IXIA1. Because the maximum limit is configured to 3, only 3 secure MAC addresses will be learned by SW1.

SW1

`#configure terminal`	Enter configure mode.
`(config)#hostname SW1`	Set the host name
`(config)#bridge 1 protocol rstp vlan-bridge`	Create a RSTP VLAN bridge on customer side
`(config)#vlan database`	Enter vlan database mode.
`(config)#vlan 2-200 bridge 1 state enable`	Configure VLAN for the bridge
`(config-vlan)#eixt`	Exit from vlan database mode.
`(config)#interface ge1`	Enter interface mode
`(config-if)#switchport`	Make the interface Layer 2
`(config-if)#bridge-group 1`	Associate the interface to bridge
`(config-if)#switchport mode hybrid`	Configure the mode as trunk
`(config-if)#switchport hybrid allowed vlan all`	Configure allowed VLAN all on the interface

(config-if)#switchport port-security	Enable port security mode dynamic
(config-if)#switchport port-security maximum 3	Limit secure MAC to 3 mac addresses.
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit interface mode
(config)#interface ge2	Enter interface mode
(config-if)#switchport	Make the interface Layer 2
(config-if)#bridge-group 1	Associate the interface to bridge
(config-if)#switchport mode hybrid	Configure the mode as trunk
(config-if)#switchport hybrid allowed vlan all	Configure allowed VLAN all on the interface
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit interface mode
(config)#logging monitor 7	Enable logging level as 7 for debugging
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit interface mode

Validation

Validation commands are `show port-security`, `show port-security interface <ifname>`, `show mac address-table count bridge 1`, `show bridge`, and `show mac address-table bridge 1`.

```
SW1#show port-security
Port    port-security mode  MAC limit CVLAN  SVLAN  static secure MAC
-------+-------------------+---------+------+------+-----------------
ge1     dynamic             3

SW1#show port-security interface ge1
Port Security Mode     : Dynamic
Secure MAC limit       : 3
Static Secure MAC list :
CVLAN  SVLAN  MAC Address
------+------+---------------

SW1#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 3
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 3

SW1#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
```

```
 1         100                  ge1         0000.0300.0500    1     100
 1         100                  ge1         0000.0300.055b    1     100
 1         100                  ge1         0000.0300.055c    1     100

SW1#show mac address-table bridge 1

CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
 100          0000.0300.0500   dynamic   ge1       Enable
 100          0000.0300.055b   dynamic   ge1       Enable
 100          0000.0300.055c   dynamic   ge1       Enable
```

Secured MAC Addresses Learned Statically

1. Stop the traffic from IXIA1 and do a `clear mac address-table dynamic bridge 1` on SW1.
2. Verify all dynamic secured MAC addresses are cleared.
3. Configure 3 static secure MAC addresses using the commands below in port security configured interface.
4. Try to add a fourth static secure MAC address.
5. Verify operator log message is displayed, saying "`port security mac limit reached`."

`(config)#interface ge1`	Enter interface mode
`(config-if)#switchport port-security mac-address 0000.0000.aaaa vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode
`(config-if)#switchport port-security mac-address 0000.0000.aaab vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode
`(config-if)#switchport port-security mac-address 0000.0000.aaac vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode
`(config-if)#commit`	Commit the candidate configuration to the running configuration.
`(config-if)#exit`	Exit interface mode

Validation

```
SW1#show port-security
Port    port-security mode  MAC limit CVLAN  SVLAN  static secure MAC
-------+-------------------+---------+------+------+-----------------
ge1     dynamic             3          100          0000.0000.aaaa
                                       100          0000.0000.aaab
                                       100          0000.0000.aaac

SW1#show port-security interface ge1
Port Security Mode     : Dynamic
Secure MAC limit       : 3
Static Secure MAC list :
CVLAN  SVLAN  MAC Address
------+------+----------------
 100          0000.0000.aaaa
 100          0000.0000.aaab
 100          0000.0000.aaac

SW1#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 0
Static (User-defined) Unicast MAC Address Count: 3
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 3

SW1#show bridge
```

```
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         100                  ge1         0000.0000.aaaa    1     -
 1         100                  ge1         0000.0000.aaab    1     -
 1         100                  ge1         0000.0000.aaac    1     -

SW1#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
100           0000.0000.aaaa  static    ge1       Enable
100           0000.0000.aaab  static    ge1       Enable
100           0000.0000.aaac  static    ge1       Enable

SW1#
```

Remove the port-security configuration method using the two commands below:

`config)#interface ge1`	Enter interface mode
`(config-if)#no switchport port-security`	Set the port-security method to static.
`(config-if)#commit`	Commit the candidate configuration to the running configuration.
`(config-if)#exit`	Exit interface mode

Static Mode

Use the below command to configure the port-security method to static and configure static secure MAC addresses using the commands in static port-security method, below.

`(config)#interface ge1`	Enter interface mode
`(config-if)#switchport port-security static`	Set the port-security method as static.
`(config-if)#switchport port-security max 3`	Limit static secure MAC to 3 mac addresses.
`(config-if)#switchport port-security mac-address 0000.0000.aaaa vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode.
`(config-if)#switchport port-security mac-address 0000.0000.aaab vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode.
`(config-if)#switchport port-security mac-address 0000.0000.aaac vlanId 100`	Add static secure MAC address for VLAN 100 in interface mode .
`(config-if)#commit`	Commit the candidate configuration to the running configuration.
`(config-if)#exit`	Exit interface mode

Verify the 3 secure static MAC addresses are added in interface ge1 using show running-config and also verify the port-security method should be static using below show commands.

Validation

```
SW1#show running-config interface ge1
interface ge1
 switchport
 bridge-group 1
 switchport mode hybrid
 switchport mode hybrid acceptable-frame-type all
 switchport hybrid allowed vlan all
 switchport port-security static
 switchport port-security maximum 3
 switchport port-security mac-address 0000.0000.aaaa vlanId 100
 switchport port-security mac-address 0000.0000.aaab vlanId 100
 switchport port-security mac-address 0000.0000.aaac vlanId 100

SW1#show port-security
Port    port-security mode  MAC limit CVLAN  SVLAN  static secure MAC
------+-------------------+---------+------+------+-----------------
ge1     static              3         100            0000.0000.aaaa
                                      100            0000.0000.aaab
                                      100            0000.0000.aaac

SW1#show port-security interface ge1
Port Security Mode     : Static
Secure MAC limit       : 3
Static Secure MAC list :
CVLAN  SVLAN  MAC Address
------+------+----------------
 100           0000.0000.aaaa
 100           0000.0000.aaab
 100           0000.0000.aaac

SW1#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 0
Static (User-defined) Unicast MAC Address Count: 3
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 3

SW1#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1         100                  ge1         0000.0000.aaaa    1     -
 1         100                  ge1         0000.0000.aaab    1     -
 1         100                  ge1         0000.0000.aaac    1     -

SW1#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
```

```
------+------+---------------+---------+---------+--------------
100           0000.0000.aaaa  static    ge1       Enable
100           0000.0000.aaab  static    ge1       Enable
100           0000.0000.aaac  static    ge1       Enable
```

Configure one more static secure MAC address on interface ge1 and try to verify "`port security mac limit reached`" operator log message is displayed.

Start sending Layer-2 traffic with incremental source MAC of 100 and with VLAN 100 from IXIA1, and verify no dynamic secure MAC addresses are being learned using all the validation commands used.

CHAPTER 18 Private VLAN Configuration

A private VLANs (PVLAN) splits a primary VLAN domain into multiple isolated broadcast sub-domains. PVLAN, also known as port isolation, is a technique where a VLAN contains switch ports that are restricted such that they can only communicate with a given uplink.

Topology

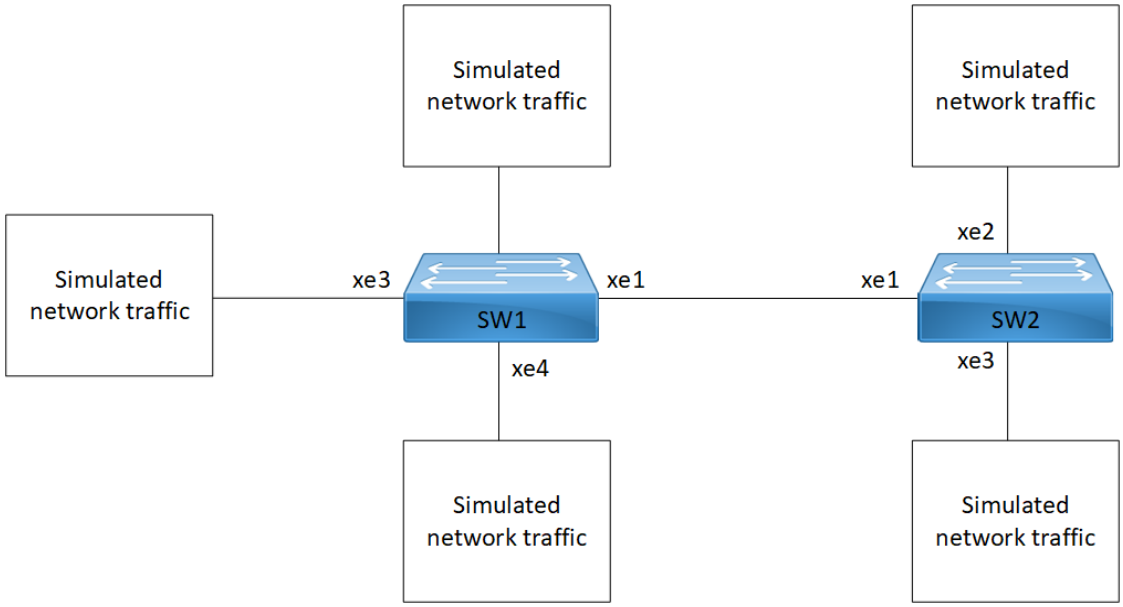


Figure 18-39: PVLAN configuration

Configure PVLAN Trunk and Promiscuous Trunk Port

SW1

`SW1#configure terminal`	Enter configuration mode
`SW1(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge
`SW1(config)#vlan database`	Enter VLAN configuration mode
`SW1(config-vlan)#vlan 10 bridge 1 state enable`	Create VLAN 10
`SW1(config-vlan)#vlan 20 bridge 1 state enable`	Create VLAN 20
`SW1(config-vlan)#vlan 100 bridge 1 state enable`	Create VLAN 100
`SW1(config-vlan)#private-vlan 10 isolated bridge 1`	Configure VLAN 10 as isolated VLAN

`SW1(config-vlan)#private-vlan 20 community bridge 1`	Configure VLAN 20 as community VLAN
`SW1(config-vlan)#private-vlan 100 primary bridge 1`	Configure VLAN 100 as primary VLAN
`SW1(config-vlan)#private-vlan 100 association add 10 bridge 1`	Associate secondary isolated VLAN 10 with primary VLAN 100
`SW1(config-vlan)#private-vlan 100association add 20 bridge 1`	Associate secondary community VLAN 20 with primary VLAN 100
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#interface xe1`	Enter interface configuration mode for xe1
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface as trunk
`SW1(config-if)#switchport trunk allowed vlan add 10,20,100`	Configure VLAN 10,20,100 (primary, secondary VLANs)
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#interface xe3`	Enter interface configuration mode for xe3
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface as trunk
`SW1(config-if)#switchport mode private-vlan promiscuous`	Configure the interface as promiscuous port for private-vlan
`SW1(config-if)#switchport trunk allowed vlan add 100`	Configure VLAN 100 (primary VLAN)
`SW1(config-if)#switchport private-vlan mapping 100 add 10`	Associate port with primary and secondary VLAN of private-vlan
`SW1(config-if)#switchport private-vlan mapping 100 add 20`	Associate port with primary and secondary VLAN of private-vlan
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#interface xe4`	Enter interface configuration mode for xe4
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode access`	Set the switching characteristics of this interface as access
`SW1(config-if)#switchport mode private-vlan host`	Configure the interface as host port for private-vlan
`SW1(config-if)#switchport access vlan 20`	Configure VLAN 20 (community VLAN)
`SW1(config-if)#switchport private-vlan host-association 100 add 20`	Associate port with primary and secondary VLAN of private-vlan
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#interface xe2`	Enter interface configuration mode for xe2
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode access`	Set the switching characteristics of this interface as access
`SW1(config-if)#switchport mode private-vlan host`	Configure the interface as host port for private-vlan

SW1(config-if)#switchport access vlan 10	Configure VLAN 10 (isolated VLAN)
SW1(config-if)#switchport private-vlan host-association 100 add 10	Associate port with primary and secondary VLAN of private-vlan
SW1(config-if)#exit	Exit interface mode
SW1(config)#commit	Commit the configure on the node.
SW1(config)#exit	Exit configuration mode

SW2

SW2#configure terminal	Enter configuration mode
SW2(config)#bridge 1 protocol ieee vlan-bridge	Create bridge
SW2(config)#vlan database	Enter VLAN configuration mode
SW2(config-vlan)#vlan 10 bridge 1 state enable	Create VLAN 10
SW2(config-vlan)#vlan 20 bridge 1 state enable	Create VLAN 20
SW2(config-vlan)#vlan 100 bridge 1 state enable	Create VLAN 100
SW2(config-vlan)#private-vlan 10 isolated bridge 1	Configure VLAN 10 as isolated VLAN
SW2(config-vlan)#private-vlan 20 community bridge 1	Configure VLAN 20 as community VLAN
SW2(config-vlan)#private-vlan 100 primary bridge 1	Configure VLAN 100 as primary VLAN
SW1(config-vlan)#private-vlan 100 association add 10 bridge 1	Associate secondary isolated VLAN 10 with primary VLAN 100
SW1(config-vlan)#private-vlan 100 association add 20 bridge 1	Associate secondary community VLAN 20 with primary VLAN 100
SW2(config-vlan)#exit	Exit VLAN configuration mode
SW2(config)#interface xe1	Enter interface configuration mode for xe1
SW2(config-if)#switchport	Configure switchport
SW2(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW2(config-if)#switchport mode trunk	Set the switching characteristics of this interface as trunk
SW2(config-if)#switchport trunk allowed vlan add 10,20,100	Configure VLAN 10,20,100 (primary, secondary VLANs)
SW2(config-if)#exit	Exit interface mode
SW2(config)#interface xe2	Enter interface configuration mode for xe2
SW2(config-if)#switchport	Configure switchport
SW2(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW2(config-if)#switchport mode access	Set the switching characteristics of this interface as access
SW2(config-if)#switchport mode private-vlan host	Configure the interface as host port for private-vlan
SW2(config-if)#switchport access vlan 10	Configure VLAN 10 (isolated VLAN)
SW2(config-if)#switchport private-vlan host-association 100 add 10	Associate port with primary and secondary VLAN of private-vlan

SW2(config-if)#exit	Exit interface mode
SW2(config)#interface xe3	Enter interface configuration mode for xe3
SW2(config-if)#switchport	Configure switchport
SW2(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW2(config-if)#switchport mode access	Set the switching characteristics of this interface as access
SW2(config-if)#switchport mode private-vlan host	Configure the interface as host port for private-vlan
SW2(config-if)#switchport access vlan 20	Configure VLAN 20 (community VLAN)
SW2(config-if)#switchport private-vlan host-association 100 add 20	Associate port with primary and secondary VLAN of private-vlan
SW2(config-if)#exit	Exit interface mode
SW2(config)#commit	Commit the configure on the node.
SW2(config)#exit	Exit configuration mode

Validation

```
SW1#show vlan private-vlan bridge 1
 PRIMARY       SECONDARY          TYPE         INTERFACES
 -------        ---------       ----------      ----------
     100              10          isolated      xe1,xe2,
     100              20         community      xe1,xe4,
SW1#
SW2#show vlan private-vlan bridge 1
 PRIMARY       SECONDARY          TYPE         INTERFACES
 -------        ---------       ----------      ----------
     100              10          isolated      xe1,xe2,
     100              20         community      xe1,xe3,
SW2#
```

Configure PVLAN Trunk and Promiscuous Access Port

SW1

SW1#configure terminal	Enter configuration mode
SW1(config)#bridge 1 protocol ieee vlan-bridge	Create bridge
SW1(config)#vlan database	Enter VLAN configuration mode
SW1(config-vlan)#vlan 10 bridge 1 state enable	Create VLAN 10
SW1(config-vlan)#vlan 20 bridge 1 state enable	Create VLAN 20
SW1(config-vlan)#vlan 100 bridge 1 state enable	Create VLAN 100

`SW1(config-vlan)#private-vlan 10 isolated bridge 1`	Configure VLAN 10 as isolated VLAN
`SW1(config-vlan)#private-vlan 20 community bridge 1`	Configure VLAN 20 as community VLAN
`SW1(config-vlan)#private-vlan 100 primary bridge 1`	Configure VLAN 100 as primary VLAN
`SW1(config-vlan)#private-vlan 100 association add 10 bridge 1`	Associate secondary isolated VLAN 10 with primary VLAN 100
`SW1(config-vlan)#private-vlan 100 association add 20 bridge 1`	Associate secondary community VLAN 20 with primary VLAN 100
`SW1(config-vlan)#exit`	Exit VLAN configuration mode
`SW1(config)#interface xe1`	Enter interface configuration mode for xe1
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode trunk`	Set the switching characteristics of this interface as trunk
`SW1(config-if)#switchport trunk allowed vlan add 10,20,100`	Configure VLAN 10,20,100 (primary, secondary VLANs)
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#interface xe3`	Enter interface configuration mode for xe3
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode access`	Set the switching characteristics of this interface as access
`SW1(config-if)#switchport mode private-vlan promiscuous`	Configure the interface as promiscuous port for private-vlan
`SW1(config-if)#switchport access vlan 100`	Configure VLAN 100 (primary VLAN)
`SW1(config-if)#switchport private-vlan mapping 100 add 10`	Associate port with primary and secondary VLAN of private-vlan
`SW1(config-if)#switchport private-vlan mapping 100 add 20`	Associate port with primary and secondary VLAN of private-vlan
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#interface xe4`	Enter interface configuration mode for xe4
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode access`	Set the switching characteristics of this interface as access
`SW1(config-if)#switchport mode private-vlan host`	Configure the interface as host port for private-vlan
`SW1(config-if)#switchport access vlan 20`	Configure VLAN 20 (community VLAN)
`SW1(config-if)#switchport private-vlan host-association 100 add 20`	Associate port with primary and secondary VLAN of private-vlan
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#interface xe2`	Enter interface configuration mode for xe2
`SW1(config-if)#switchport`	Configure switchport
`SW1(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW1(config-if)#switchport mode access`	Set the switching characteristics of this interface as access

`SW1(config-if)#switchport mode private-vlan host`	Configure the interface as host port for private-vlan
`SW1(config-if)#switchport access vlan 10`	Configure VLAN 10 (isolated VLAN)
`SW1(config-if)#switchport private-vlan host-association 100 add 10`	Associate port with primary and secondary VLAN of private-vlan
`SW1(config-if)#exit`	Exit interface mode
`SW1(config)#commit`	Commit the configure on the node.
`SW1(config)#exit`	Exit configuration mode

SW2

`SW2#configure terminal`	Enter configuration mode
`SW2(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge
`SW2(config)#vlan database`	Enter VLAN configuration mode
`SW2(config-vlan)#vlan 10 bridge 1 state enable`	Create VLAN 10
`SW2(config-vlan)#vlan 20 bridge 1 state enable`	Create VLAN 20
`SW2(config-vlan)#vlan 100 bridge 1 state enable`	Create VLAN 100
`SW2(config-vlan)#private-vlan 10 isolated bridge 1`	Configure VLAN 10 as isolated VLAN
`SW2(config-vlan)#private-vlan 20 community bridge 1`	Configure VLAN 20 as community VLAN
`SW2(config-vlan)#private-vlan 100 primary bridge  1`	Configure VLAN 100 as primary VLAN
`SW1(config-vlan)#private-vlan 100 association add 10 bridge 1`	Associate secondary isolated VLAN 10 with primary VLAN 100
`SW1(config-vlan)#private-vlan 100 association add 20 bridge 1`	Associate secondary community VLAN 20 with primary VLAN 100
`SW2(config-vlan)#exit`	Exit VLAN configuration mode
`SW2(config)#interface xe1`	Enter interface configuration mode for xe1
`SW2(config-if)#switchport`	Configure switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode trunk`	Set the switching characteristics of this interface as trunk
`SW2(config-if)#switchport trunk allowed vlan add 10,20,100`	Configure VLAN 10,20,100 (primary, secondary VLANs)
`SW2(config-if)#exit`	Exit interface mode
`SW2(config)#interface xe2`	Enter interface configuration mode for xe2
`SW2(config-if)#switchport`	Configure switchport
`SW2(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`SW2(config-if)#switchport mode access`	Set the switching characteristics of this interface as access
`SW2(config-if)#switchport mode private-vlan host`	Configure the interface as host port for private-vlan
`SW2(config-if)#switchport access vlan 10`	Configure VLAN 10 (isolated VLAN)

SW2(config-if)#switchport private-vlan host-association 100 add 10	Associate port with primary and secondary VLAN of private-vlan
SW2(config-if)#exit	Exit interface mode
SW2(config)#interface xe3	Enter interface configuration mode for xe3
SW2(config-if)#switchport	Configure switchport
SW2(config-if)#bridge-group 1	Associate interface with bridge-group 1
SW2(config-if)#switchport mode access	Set the switching characteristics of this interface as access
SW2(config-if)#switchport mode private-vlan host	Configure the interface as host port for private-vlan
SW2(config-if)#switchport access vlan 20	Configure VLAN 20 (community VLAN)
SW2(config-if)#switchport private-vlan host-association 100 add 20	Associate port with primary and secondary VLAN of private-vlan
SW2(config-if)#exit	Exit interface mode
SW2(config)#commit	Commit the configure on the node.
SW2(config)#exit	Exit configuration mode

Validation

```
SW1#show vlan private-vlan bridge 1
 PRIMARY       SECONDARY          TYPE          INTERFACES
 -------        ---------       ----------      ----------
     100              10          isolated      xe1,xe2,
     100              20         community      xe1,xe4,

SW2#show vlan private-vlan bridge 1
 PRIMARY       SECONDARY          TYPE          INTERFACES
 -------        ---------       ----------      ----------
     100              10          isolated      xe1,xe2,
     100              20         community      xe1,xe3,
SW2#
```

Traffic Validation

Configure Host trunk and promiscuous trunk configurations on SW1 and SW2

1. Send untagged traffic from SW1 xe3 (promiscuous port), traffic should forward to interfaces xe1,xe2, and xe4. On SW2, traffic should receive from xe1 and forward through xe2 and xe3.

```
SW1#show interface counters rate mbps
+------------------+-------------+-------------+-------------+-------------+
|     Interface    |    Rx mbps  |    Rx pps   |    Tx mbps  |    Tx pps   |
+------------------+-------------+-------------+-------------+-------------+
 xe1                0.00          0             86.49         84462
 xe2                0.00          0             86.49         84462
 xe3                86.49         84462         0.00          0
 xe4                0.00          0             86.49         84462

SW2#show interface counters rate mbps
```

```
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe1                 86.49          84462         0.00           0
 xe2                 0.00           0             86.49          84462
 xe3                 0.00           0             86.49          84462
```

2. Send untagged traffic from SW1 xe2 (isolated port), traffic should forward to interfaces xe3 and xe1. On SW2, traffic should receive from xe1 and remaining ports should be 0.

```
SW1#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe1                 0.00           0             86.49          84462
 xe2                 86.49          84462         0.00           0
 xe3                 0.00           0             86.49          84462
 xe4                 0.00           0             0.00           0

SW2#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe1                 86.49          84462         0.00           0
 xe2                 0.00           0             0.00           0
 xe3                 0.00           0             0.00           0
```

3. Send untagged traffic from SW1 xe4 (community port), traffic should forward through interfaces xe3 and xe1. On SW2, traffic should receive from xe1 and forward to xe3.

```
SW1#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe1                 0.00           0             86.49          84462
 xe2                 0.00           0             0.00           0
 xe3                 0.00           0             86.49          84462
 xe4                 86.49          84462         0.00           0

SW2#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe1                 86.49          84462         0.00           0
 xe2                 0.00           0             0.00           0
 xe3                 0.00           0             86.49          84462
```

CHAPTER 19 Layer 2 Subinterface Configuration

This chapter contains examples of configuring L2 Subinterfaces.

A single physical interface when required to handle multiple VLAN traffic, can be divided into multiple logical interfaces called sub-interfaces.

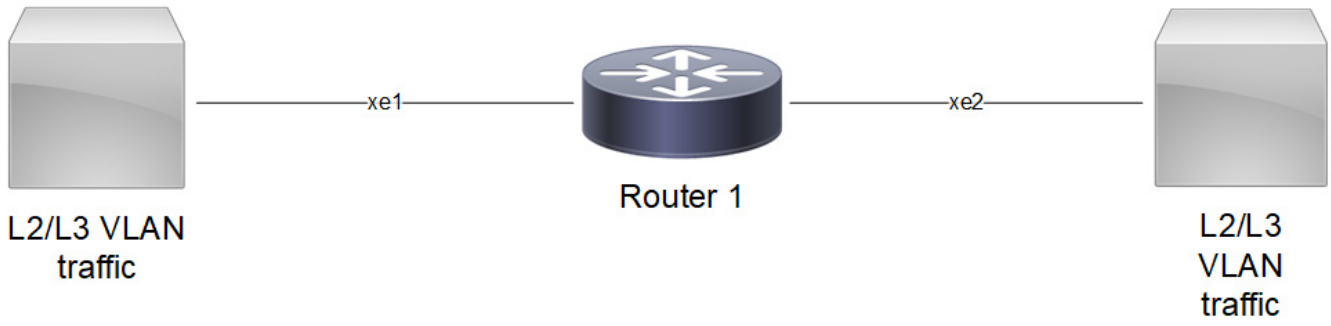
All sub-interfaces under the physical port will use their parent port for sending and receiving data.

Sub-interfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN identifiers. Because VLANs allow you to keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces.

Note: Refer to the release note for features supported by L2 Sub-interface.

Topology

Below figure shows and example of subinterface configuration for one node with cross-connect. In this example, there is one router R1 with 2 connections



The xe1.10 and xe2.10 subinterface is created on R1

Sub-interface can be created over physical or LAG interfaces.

Note: Use `dot1ad ethertype` (0x8100 | 0x88a8 | 0x9100 | 0x9200) command to configure the service-tpid value on parent port of a subinterface. By this the tpid used for service tag for a subinterface may be inherited from the one applied to parent interface.

Note: For any dot1ad subinterface to be functional, `dot1ad ethertype` should be set to desired value as 0x88a8/ 0x9100/0x9200. Default value is 8100. To verify the ethertype value for the interface use show interface <subinterface> command.

Configure L2 Subinterface with cross-connect

`#configure terminal`	Enter configure mode.
`(config)#interface xe1`	Enter interface mode

(config-if)# dot1ad ethertype 0x88a8	Configure interface with tpid value as 88a8
(config-if)#exit	Exit interface mode.
(config)#interface xe1.10 switchport	Creates a L2 sub-interface as xe1.10
(config-if)#encapsulation dot1q 10	Configure the encapsulation as dot1q matching vlan 10
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode
(config-if)# dot1ad ethertype 0x88a8	Configure interface with tpid value as 88a8
(config-if)#exit	Exit interface mode.
(config-if)#interface xe2.10 switchport	Creates a L2 sub-interface as xe2.10
(config-if)#encapsulation dot1q 10	Configure the encapsulation as dot1q matching vlan 10
(config-if)#exit	Exit interface mode.
(config)# cross-connect CC1	Create cross-connect with name CC1
(config-xc)# interface xe1.10	Attach interface xe1.10
(config-xc)# interface xe2.10	Attach interface xe2.10
(config-xc)#exit	Exit cross-connect mode.
(config)#commit	Commit the transaction.

Configure L2 Subinterface(Double-Push) with cross-connect

#configure terminal	Enter configure mode.
(config)#interface xe1.10 switchport	Creates a L2 sub-interface as xe1.10
(config-if)#encapsulation untagged	Configure the encapsulation as untagged
(config-if)# rewrite push 0x8100 200 inner-dot1q 200	Configure rewrite push with inner vlan 200 and outer vlan 200
(config-if)#exit	Exit interface mode
(config)#interface xe2.10 switchport	Creates a L2 sub-interface as xe2.10
(config-if)# encapsulation dot1ad 200 inner-dot1q 200	Configure the encapsulation with inner vlan 200 and outer vlan 200
(config-if)#exit	Exit interface mode
(config)# cross-connect CC1	Create cross-connect with name CC1
(config-xc)# interface xe1.10	Attach interface xe1.10
(config-xc)# interface xe2.10	Attach interface xe2.10
(config-xc)#exit	Exit cross-connect mode.
(config)#commit	Commit the transaction.

Configure L2 Subinterface(Double-Pop) with cross-connect

#configure terminal	Enter configure mode.
(config)##interface xe1.10 switchport	Creates a L2 sub-interface as xe1.10

(config-if)#encapsulation untagged	Configure the encapsulation as untagged
(config-if)#exit	Exit interface mode
(config)#interface xe2.10 switchport	Creates a L2 sub-interface as xe2.10
(config-if)# encapsulation dot1ad 200 inner-dot1q 200	Configure the encapsulation with inner vlan 200 and outer vlan 200
(config-if)# rewrite pop-2tag	Configure rewrite pop-2tag
(config-if)#exit	Exit interface mode
(config)# cross-connect CC1	Create cross-connect with name CC1
(config-xc)# interface xe1.10	Attach interface xe1.10
(config-xc)# interface xe2.10	Attach interface xe2.10
(config-xc)#exit	Exit cross-connect mode.
(config)#commit	Commit the transaction.

Creating a Subinterface with Encapsulation

Single encapsulation as dot1q with vlan range

```
configure terminal (config)#interface xe1.100 switchport
(config-if)# encapsulation dot1q 100-200
```

Single encapsulation as dot1ad with vlan range

```
configure terminal (config)#interface xe1.100 switchport
(config-if)# encapsulation dot1ad 100-200
```

Double encapsulation as dot1q

```
configure terminal (config)#interface xe1.100 switchport
(config-if)# encapsulation dot1q 10 inner-dot1q 10
```

Double encapsulation as dot1ad

```
configure terminal (config)#interface xe1.200 switchport
(config-if)# encapsulation dot1ad 20 inner-dot1q 20
```

Encapsulation as default

```
configure terminal (config)#interface xe1.101 switchport
(config-if)# encapsulation default
```

Encapsulation as untagged

```
configure terminal (config)#interface xe1.102 switchport
(config-if)# encapsulation untagged
```

Rewrite with push

```
configure terminal (config)#interface xe1.10 switchport
(config-if)# encapsulation dot1q 10
(config-if)# rewrite push 0x8100 100
(config-if)#interface xe2.20 switchport
(config-if)# encapsulation dot1q 100 inner-dot1q 10
(config-if)#exit
(config)# cross-connect CC1
```

```
(config-xc)# interface xe1.10
(config-xc)# interface xe2.10
```

Note: For incoming traffic at sub-interface “interface IFNAME”, the "rewrite push" will add VLAN tag with TPID values 8100.

Note: For outgoing traffic at sub-interface "interface IFNAME", the "rewrite push" will pop the VLAN. The egress pop removes whatever outer VLAN tag is present, regardless of its value. This is not restricted to VLAN 100.

Rewrite with translate

```
configure terminal (config)# interface xe1
(config-if)# dot1ad ethertype 0x9100
(config-if)#interface xe1.10 switchport
(config-if)# encapsulation dot1ad 200
(config-if)# rewrite translate 1-to-1 0x9100 100
(config-if)#interface xe2
(config-if)# dot1ad ethertype 0x9100
(config-if)#interface xe2.20 switchport
(config-if)# encapsulation dot1ad 100
(config-if)#exit
(config)# cross-connect CC1
(config-xc)# interface xe1.10
(config-xc)# interface xe2.10
```

Note: For incoming and outgoing traffic at sub-interface “interface IFNAME”, the "rewrite translate" will update VLAN tag with TPID values 9100.

Rewrite with pop

```
#configure terminal (config)#interface xe1.10 switchport
(config-if)# encapsulation dot1q 100
(config-if)# rewrite pop
(config-if)#interface xe2.20 switchport
(config-if)# encapsulation untagged
(config-if)#exit
(config)# cross-connect CC1
(config-xc)# interface xe1.10
(config-xc)# interface xe2.10
```

Note: For incoming traffic at sub-interface “interface IFNAME”, the "rewrite pop" will pop the vlan.

Note: For outgoing traffic at sub-interface “interface IFNAME”, the "rewrite pop" will add VLAN tag with TPID values 8100.

Note: Push, pop and translate rewrite operations are supported with tpid values 8100/88a8/9100/9200 as symmetric operation.

No subinterfaces

```
#configure terminal (config)#interface xe1
(config-if)# no subinterfaces
```

Note: no Subinterfaces will remove all the Subinterfaces.

Note: Same physical interface will support both L2 and L3 subinterfaces.

L2SI Statistics

Enable below commands to get L2SI statistics

```
#configure terminal (config)# hardware-profile statistics ac-lif enable
```

Note: Reload the node, and then only statistics command will get effective.

Verification commands

Subinterfaces appear as any physical interface in the show running-config or the show ip interface brief output and can be configured as any other interface.

The following examples display subinterface information from various show commands.

show interface brief

```
R1#show interface brief | include xe1
xe1        ETH   --    routed            up      none    10g   --
xe1.10        SUBINTERFACE     up      --     N/A
```

show interface <>

```
R1#show interface xe1.10
Interface xe1.10
  Hardware is SUBINTERFACE  Current HW addr: b86a.97d0.25c5
  Physical:(Not Applicable)  Logical:(not set)
  Port Mode is Switch
  Interface index: 20484106
  Metric 1
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Encapsulation Dot1q (0x8100) Virtual LAN
  Outer Match: Dot1q VLAN 10
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
  Bandwidth 1g
  DHCP client is disabled.
  Last Flapped: Never
  Statistics last cleared: Never
  RX
    unicast packets 0 multicast packets 0 broadcast packets 0
    input packets 0 bytes 0
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 0 broadcast packets 0
    output packets 0 bytes 0
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0
```

show cross-connect

```
R1#show cross-connect
cross-connect status
XC name                         Ep1              Ep2              Status
-------------------------------+----------------+----------------+-------
CC1                             xe1.10           xe2.10           UP
-------------------------------+----------------+----------------+-------
AC cross-connect summary
Total : 1
Up    : 1
Down  : 0
R1#show running-config interface xe1
!
interface xe1
 dot1ad ethertype 0x88a8
!
R1#show run interface xe1.10
!
interface xe1.10 switchport
 encapsulation dot1q 10
 rewrite push 0x8100 10
!
R1#show running-config interface xe1
!
interface xe2
 dot1ad ethertype 0x88a8
!
R1#show run interface xe2.10
!
interface xe2.10 switchport
 encapsulation dot1q 10
!
```

show interface xe1.10 counters

```
R1#show interface xe1.10 counters
Interface xe1.10
Rx Packets: 50000
Rx Bytes: 50000000
R1#show interface xe2.10 counters
Interface xe2.10
Tx Packets: 50000
Tx Bytes: 49900000
```

CHAPTER 20 Layer 2 EPL and EVPL Configuration

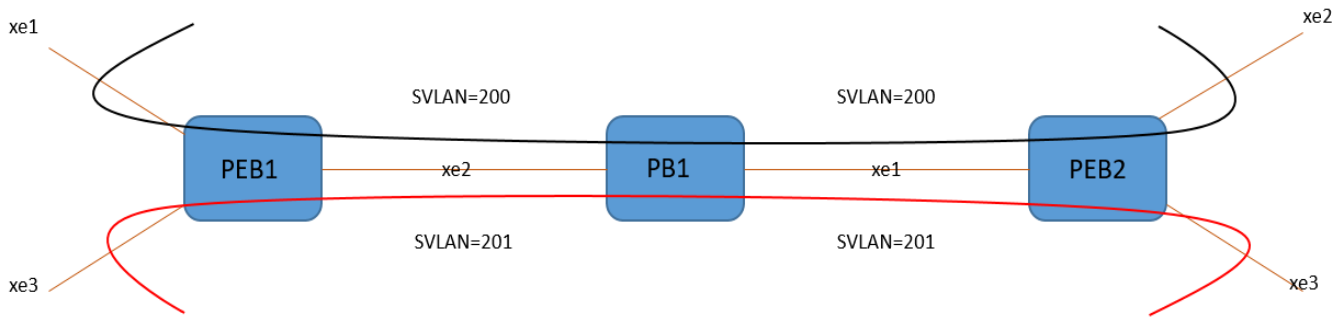
This chapter contains examples of configuring L2 EPL and EVPL Subinterfaces.

Ethernet Private Line (EPL) and Ethernet Virtual Private Line (EVPL) are Ethernet services standardized by the Metro Ethernet Forum (MEF) under the category of 'E-Line' services. Both EPL and EVPL offer the advantages of private, high-speed connections with the added flexibility and scalability provided by Multiprotocol Label Switching (MPLS) technology. They are designed to operate across a range of bandwidths to meet diverse business requirements. The key distinction between EPL and EVPL lies in their configuration and how they handle network connections.

- EPL provides a Point-to-Point (P2P) connection between two dedicated User Network Interfaces (UNIs). This setup offers a high degree of transparency and is ideal for businesses requiring a simple and direct link between two locations.
- EVPL enables multiple Ethernet Virtual Connections (EVCs) per UNI, supporting Point-to-MultiPoint (P2MP) connectivity through service multiplexing. This allows businesses to establish a one-to-many network topology, where a single UNI can connect to multiple remote sites, providing greater flexibility in network design.

Topology

Below figure shows the EPL configuration:



Configure L2 EPL

PEB1

`#configure terminal`	Enter configure mode.
`(config)#interface xe1`	Enter interface mode
`(config-if)# dot1ad ethertype 0x88a8`	Configure interface with tpid value as 88a8
`(config-if)#interface xe1.200 switchport`	Creates a L2 sub-interface as xe1.200
`(config-if)#encapsulation deafult`	Configure the encapsulation as default
`(config-if)# rewrite push 0x8100 200`	Configure rewrite push with vlan 200
`(config-if)#exit`	Exit interface mode.

(config)#interface xe2	Enter interface mode
(config-if)# dot1ad ethertype 0x88a8	Configure interface with tpid value as 88a8
(config-if)#interface xe2.200 switchport	Creates a L2 sub-interface as xe2.10
(config-if)#encapsulation dot1q 200	Configure the encapsulation as dot1q matching vlan 200
(config-if)#exit	Exit interface mode.
(config)# cross-connect PEB-1 200	Create cross-connect with name PEB1-200
(config-xc)# interface xe1.200	Attach interface xe1.10
(config-xc)# interface xe2.200	Attach interface xe2.10
(config)#interface xe3	Enter interface mode
(config-if)# dot1ad ethertype 0x88a8	Configure interface with tpid value as 88a8
(config-if)#interface xe3.201 switchport	Creates a L2 sub-interface as xe3.201
(config-if)#encapsulation deafult	Configure the encapsulation as default
(config-if)# rewrite push 0x8100 201	Configure rewrite push with vlan 201
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode
(config-if)#interface xe2.201 switchport	Creates a L2 sub-interface as xe2.201
(config-if)#encapsulation dot1q 201	Configure the encapsulation as dot1q matching vlan 201
(config)# cross-connect PEB1-201	Create cross-connect with name PEB1-201
(config-xc)# interface xe3.201	Attach interface xe3.201
(config-xc)# interface xe2.201	Attach interface xe2.201
(config-if)#exit	Exit interface mode.

PB1

#configure terminal	Enter configure mode.
(config)#interface xe2	Enter interface mode
(config-if)# dot1ad ethertype 0x88a8	Configure interface with tpid value as 88a8
(config-if)#interface xe2.200 switchport	Creates a L2 sub-interface as xe2.200
(config-if)#encapsulation dot1ad 200	Configure the encapsulation vlan 200
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode
(config-if)# dot1ad ethertype 0x88a8	Configure interface with tpid value as 88a8
(config-if)#interface xe1.200 switchport	Creates a L2 sub-interface as xe1.200
(config-if)#encapsulation dot1ad 200	Configure the encapsulation as dot1ad matching vlan 200
(config-if)#exit	Exit interface mode.
(config)# cross-connect PB1-200	Create cross-connect with name PB1-200
(config-xc)# interface xe2.200	Attach interface xe2.200
(config-xc)# interface xe1.200	Attach interface xe1.200
(config)#interface xe2	Enter interface mode
(config-if)# dot1ad ethertype 0x88a8	Configure interface with tpid value as 88a8

(config-if)#interface xe2.201 switchport	Creates a L2 sub-interface as xe2.201
(config-if)#encapsulation dot1ad 201	Configure the encapsulation as dot1ad with vlan 201
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter interface mode
(config-if)#interface xe1.201 switchport	Creates a L2 sub-interface as xe1.201
(config-if)#encapsulation dot1ad 201	Configure the encapsulation as dot1ad with vlan 201
(config-if)#exit	Exit interface mode.
(config)# cross-connect PB1-201	Create cross-connect with name PEB1-201
(config-xc)# interface xe1.201	Attach interface xe1.201
(config-xc)# interface xe2.201	Attach interface xe2.201
(config-if)#exit	Exit interface mode.

PB1

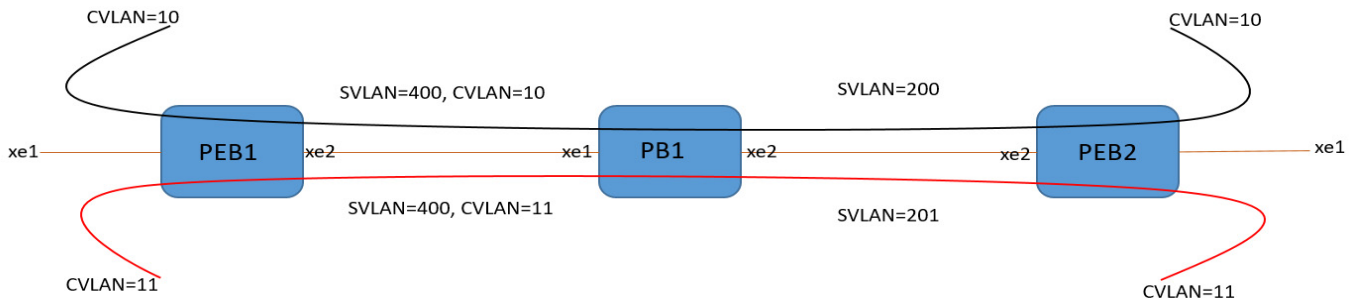
#configure terminal	Enter configure mode.
(config)#interface xe1	Enter interface mode
(config-if)# dot1ad ethertype 0x88a8	Configure interface with tpid value as 88a8
(config-if)#interface xe1.200 switchport	Creates a L2 sub-interface as xe1.200
(config-if)#encapsulation dot1ad 200	Configure the encapsulation as dot1ad 200
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode
(config-if)# dot1ad ethertype 0x88a8	Configure interface with tpid value as 88a8
(config-if)#interface xe2.200 switchport	Creates a L2 sub-interface as xe2.200
(config-if)#encapsulation default	Configure the encapsulation as default
(config-if)# rewrite push 0x88a8 200	Configure rewrite push with vlan 200
(config-if)#exit	Exit interface mode.
(config)# cross-connect PEB2-200	Create cross-connect with name CC1
(config-xc)# interface xe1.200	Attach interface xe1.200
(config-xc)# interface xe2.200	Attach interface xe2.200
(config)#interface xe1	Enter interface mode
(config-if)#interface xe1.201 switchport	Creates a L2 sub-interface as xe1.201
(config-if)#encapsulation dot1ad 201	Configure the encapsulation as dot1ad with vlan 201
(config-if)#exit	Exit interface mode.
(config)#interface xe3	Enter interface mode
(config-if)# dot1ad ethertype 0x88a8	Configure interface with tpid value as 88a8
(config-if)#interface xe3.201 switchport	Creates a L2 sub-interface as xe3.201
(config-if)#encapsulation default	Configure the encapsulation as default
(config-if)# rewrite push 0x88a8 201	Configure rewrite push with vlan 201
(config-if)#exit	Exit interface mode.
(config)# cross-connect PEB2-201	Create cross-connect with name CC1

`(config-xc)# interface xe1.201`	Attach interface xe1.201
`(config-xc)# interface xe3.201`	Attach interface xe3.201
`(config-if)#exit`	Exit interface mode.

Configure L2 EVPL

Topology

Below figure shows the EVPL configuration:



PEB1

SERVICE Configuration (SVLAN=400, CVLAN=10 and SVLAN=400, CVLAN=11

)

`#configure terminal`	Enter configure mode.
`(config)#interface xe1`	Enter interface mode
`(config-if)# dot1ad ethertype 0x88a8`	Configure interface with tpid value as 88a8
`(config-if)#interface xe1.10 switchport`	Creates a L2 sub-interface as xe1.10
`(config-if)#encapsulation dot1q 10`	Configure the encapsulation as default
`(config-if)# rewrite push 0x88a8 400`	Configure rewrite push with vlan 400
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter interface mode
`(config-if)# dot1ad ethertype 0x88a8`	Configure interface with tpid value as 88a8
`(config-if)#interface xe2.400 switchport`	Creates a L2 sub-interface as xe2.400
`(config-if)#encapsulation dot1ad 400`	Configure the encapsulation as dot1ad matching vlan 400
`(config-if)#exit`	Exit interface mode.
`(config)# cross-connect PEB1-400-10`	Create cross-connect with name CC1
`(config-xc)# interface xe1.10`	Attach interface xe1.10
`(config-xc)# interface xe2.400`	Attach interface xe2.400
`(config)#interface xe1`	Enter interface mode
`(config-if)#interface xe1.11 switchport`	Creates a L2 sub-interface as xe1.11

(config-if)#encapsulation dot1q 11	Configure the encapsulation as dot1q matching vlan 11
(config-if)# rewrite push 0x88a8 400	Configure rewrite push with vlan 400
(config-if)#exit	Exit interface mode.
(config)# cross-connect PEB1-400-11	Create cross-connect with name CC1
(config-xc)# interface xe1.11	Attach interface xe1.11
(config-xc)# interface xe2.400	Attach interface xe2.400
(config-if)#exit	Exit interface mode.

PB1

PB Transport Configuration

#configure terminal	Enter configure mode.
(config)#interface xe1	Enter interface mode
(config-if)# dot1ad ethertype 0x88a8	Configure interface with tpid value as 88a8
(config-if)#interface xe1.400 switchport	Creates a L2 sub-interface as xe1.10
(config-if)#encapsulation dot1ad 400	Configure the encapsulation as dot1ad matching vlan 400
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode
(config-if)# dot1ad ethertype 0x88a8	Configure interface with tpid value as 88a8
(config-if)#interface xe2.400 switchport	Creates a L2 sub-interface as xe2.400
(config-if)#encapsulation dot1ad 400	Configure the encapsulation as dot1ad matching vlan 400
(config-if)#exit	Exit interface mode.
(config)# cross-connect PB1-400	Create cross-connect with name CC1
(config-xc)# interface xe1.400	Attach interface xe1.400
(config-xc)# interface xe2.400	Attach interface xe2.400
(config-if)#exit	Exit interface mode.

PEB2

SERVICE Configuration (SVLAN=400, CVLAN=10 and SVLAN=400, CVLAN=11)

#configure terminal	Enter configure mode.
(config)#interface xe1	Enter interface mode
(config-if)# dot1ad ethertype 0x88a8	Configure interface with tpid value as 88a8
(config-if)#interface xe1.10 switchport	Creates a L2 sub-interface as xe1.10
(config-if)#encapsulation dot1q 10	Configure the encapsulation as dot1q matching vlan 10
(config-if)# rewrite push 0x88a8 400	Configure rewrite push with vlan 400
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode
(config-if)# dot1ad ethertype 0x88a8	Configure interface with tpid value as 88a8
(config-if)#interface xe2.400 switchport	Creates a L2 sub-interface as xe2.400

(config-if)#encapsulation dot1ad 400	Configure the encapsulation as dot1ad matching vlan 400
(config-if)#exit	Exit interface mode.
(config)# cross-connect PEB2-400-10	Create cross-connect with name CC1
(config-xc)# interface xe1.10	Attach interface xe1.10
(config-xc)# interface xe2.400	Attach interface xe2.400
(config)#interface xe1	Enter interface mode
(config-if)#interface xe1.11 switchport	Creates a L2 sub-interface as xe1.11
(config-if)#encapsulation dot1q 11	Configure the encapsulation as dot1q matching vlan 11
(config-if)# rewrite push 0x88a8 400	Configure rewrite push with vlan 400
(config-if)#exit	Exit interface mode.
(config)# cross-connect PEB2-400-11	Create cross-connect with name PEB2-400-11
(config-xc)# interface xe1.11	Attach interface xe1.11
(config-xc)# interface xe2.400	Attach interface xe2.400
(config-if)#exit	Exit interface mode.

Verification commands

The following examples display L2 EPL And EVPL information from various show commands.

show interface brief

```
PEB1#show interface brief | include xe2
xe2           ETH           --    routed           up      none    10g   --       No  No
xe2.200       SUBINTERFACE  --    --               up      none    10g   --       No  No
xe2.201       SUBINTERFACE  --    --               up      none    10g   --       No  No
PEB1#
PEB1#
PEB1#show interface brief | include xe1
xe1          ETH           --    routed           up      none    10g   --       No  No
xe1.201      SUBINTERFACE  --    --               up      none    10g   --       No  No
PEB1#
PEB1#show interface brief | include xe3
xe3           ETH           --    routed           up      none    10g   --       No  No
xe3.200       SUBINTERFACE  --    --               up      none    10g   --       No  No
```

show interface <>

```
PEB1#sh interface xe2.200
Interface xe2.200
  Hardware is SUBINTERFACE  Current HW addr: e8c5.7a90.d9c8
  Physical:e8c5.7a90.d9c8  Logical:(not set)
  Port Mode is Switch
  Interface index: 327909576
  GMPLS index: 56
  Metric 1 mtu 1500  link-speed 10g
  Debounce timer: disable
  <UP,BROADCAST,RUNNING,ALLMULTI,MULTICAST>
```

```
  VRF Binding: Not bound
  Encapsulation Dot1q (0x8100) Virtual LAN
  Outer Match: Dot1q VLAN 200
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
 Extended-Admin-Group(s): None
  Bandwidth 10g
  DHCP client is disabled.
  Last Flapped: Never
  Statistics last cleared: Never
  RX
    unicast packets 0 multicast packets 0 broadcast packets 0
    input packets 0 bytes 0
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 0 broadcast packets 0
    output packets 0 bytes 0
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0
```

show cross-connect

```
PEB1#show cross-connect
cross-connect status
XC name                         Ep1              Bkp-Ep1          Ep2              Bkp-
Ep2          Status
-----------------------------+----------------+----------------+----------------+------
----------+-------
PEB-1-200                   xe4.200         -             xe6.200         -
UP
PEB1-201                    xe11.201        -             xe6.201         -
UP
-----------------------------+----------------+----------------+----------------+------
----------+-------
AC cross-connect summary
Total : 2
Up    : 2
Down  : 0
!
```

show interface xe1.200 counters

```
PEB1:
PEB1#show interface xe2.200 counters
Interface xe2.200
  Tx Packets: 50000
  Tx Bytes: 50000000
```

```
PEB1#show interface xe1.200 counters
Interface xe1.200
  Tx Packets: 50000
  Tx Bytes: 50000000
PEB1#show interface xe2.201 counters
Interface xe2.201
  Tx Packets: 50000
  Tx Bytes: 50000000
PEB1#show interface xe3.201 counters
Interface xe3.201
  Tx Packets: 50000
  Tx Bytes: 50000000
```

CHAPTER 21 Bridging Support Over Layer2 Sub-interface

Overview

Bridge-domain bridging allows Layer 2 switching across multiple sub-interfaces. Each sub-interface, configured with encapsulation dot1q, becomes part of a common bridge-domain. This setup enables an Ethernet LAN (ELAN)-like service across sub-interfaces.

Feature Characteristics

- Supports Layer 2 switching between sub-interfaces on the same or different physical interfaces.
- Uses 802.1Q VLAN tagging for traffic separation and identification.
- Provides BUM traffic flooding within the bridge-domain.
- Dynamically learns MAC addresses for known unicast forwarding.
- Static MAC address support for deterministic forwarding.

NETCONF Support for Dynamic MAC Addresses

- NETCONF support fetches dynamically learned MAC address entries, mirroring the output of the show mac address-table bridge-domain command. Each entry includes:
  - The dynamically learned MAC address via traffic.
  - The interface (port or sub-interface) where the MAC was learned.
  - The bridge-domain identifier in which the MAC entry belongs.
- The XPath `/network-instances/network-instance/bridge-domain/bridge-domain-mac-table/dynamic-entry` indicates the NETCONF data path used to fetch dynamically learned MAC address entries associated with a bridge-domain instance on the device.
- The XPath `/network-instances/network-instance/bridge-domain/bridge-domain-mac-table/static-entry` aligns with the separation of dynamic and static entries, ensuring clear organization of bridge-domain MAC tables.

Benefits

- Simplifies service delivery for ELAN or pseudo-wire services.
- Reduces flooding through MAC learning and static mapping.
- Enhance traffic control with static MAC configurations.
- Allows flexible service mapping using sub-interfaces instead of full physical ports.

Prerequisites

- Interfaces must support Layer 2 mode and be capable of sub-interface configuration.
- VLANs must be correctly assigned and unique across sub-interfaces.

- Bridge-domain must be defined and interfaces added to it.

Configuration

The following steps outline how to configure Layer 2 sub-interfaces, encapsulation types, rewrite operations, and bridge domains on OcNOS for various L2 service scenarios.

Topology

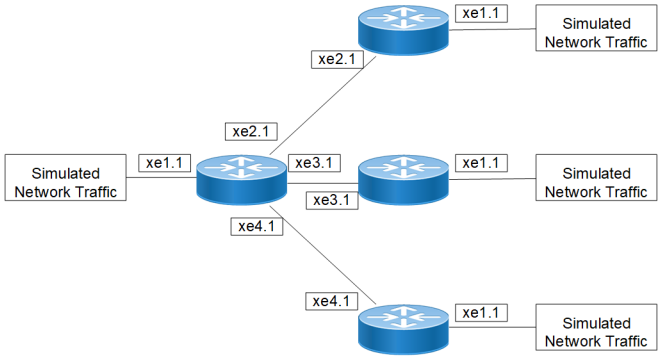


Figure 21-40: Bridging support over L2 sub-interface

Configuring Layer 2 Sub-interfaces and Bridge Domain

1. **Configure Physical Interface for Dot1ad**

   Set the TPID value to 0x88a8, enabling support for 802.1ad (Q-in-Q) encapsulation on the physical interface.

```
#configure terminal
(config)#interface xe1
(config-if)#dot1ad ethertype 0x88a8
(config-if)#exit

(config)#interface xe2
(config-if)#dot1ad ethertype 0x88a8
(config-if)#exit
```

2. **Create Sub-Interfaces and Apply Encapsulation**

   Create a Layer 2 sub-interfaces (`xe1.1 and xe2.1`) and configure it to match traffic tagged with VLAN ID 10 using 802.1Q encapsulation.

```
(config)#interface xe1.1 switchport
(config-if)#encapsulation dot1q 10
(config-if)#exit

(config)#interface xe2.1 switchport
(config-if)#encapsulation dot1q 10
(config-if)#exit
```

3. **Create Bridge Domain and Attach Interfaces**

Create Bridge Domain 1 and attach sub-interfaces `xe1.1` and `xe2.1` to it, enabling Layer 2 bridging between them.

```
(config)#bridge-domain 1
(config-bridge-domain)#interface xe1.1
(config-bridge-domain)#interface xe2.1
(config-bridge-domain)#exit
(config)#commit
```

Configuring L2 Sub-interface with Double-Push and Bridge Domain

1. Create and Configure Double-Push Rewrite

- Create the sub-interface `xe1.1` and configure it to accept untagged frames from the customer-facing side (typically access-facing). This sets up the interface to apply tagging before forwarding.
- Configure the interface to push two VLAN tags, both outer and inner set to `VLAN 200` with `TPID 0x8100`. This is commonly used for Q-in-Q tunneling where the provider edge applies double tagging to customer traffic.

```
#configure terminal
(config)#interface xe1.1 switchport
(config-if)#encapsulation untagged
(config-if)#rewrite push 0x8100 200 inner-dot1q 200
(config-if)#exit
```

- Configure the sub-interface `xe2.1` to match traffic with two VLAN tags (outer `802.1ad VLAN 200` and inner `VLAN 200`).

```
(config)#interface xe2.1 switchport
(config-if)#encapsulation dot1ad 200 inner-dot1q 200
(config-if)#exit
```

2. Add Interfaces to Bridge Domain

Create Bridge Domain 1 and attach sub-interfaces `xe1.1` and `xe2.1` to it, enabling Layer 2 bridging between them.

```
(config)#bridge-domain 1
(config-bridge-domain)#interface xe1.1
(config-bridge-domain)#interface xe2.1
(config-bridge-domain)#exit
(config)#commit
```

Configuring L2 Sub-interface with Double-Pop and Bridge Domain

1. Create Sub-Interfaces and Rewrite with Pop

- Set `xe1.1` to receive untagged traffic. This usually represents the access or customer side that does not use VLAN tagging.

```
#configure terminal
(config)#interface xe1.1 switchport
(config-if)#encapsulation untagged
(config-if)#exit
```

- Configure `xe2.1` to match traffic with two VLAN tags (outer 802.1ad VLAN 200 and inner VLAN 200) and pop both tags before forwarding.

```
(config)#interface xe2.1 switchport
(config-if)#encapsulation dot1ad 200 inner-dot1q 200
(config-if)#rewrite pop-2tag
(config-if)#exit
```

2. Add Interfaces to Bridge Domain

Create Bridge Domain 1 and attach sub-interfaces `xe1.1` and `xe2.1` to it, enabling Layer 2 bridging between them.

```
(config)#bridge-domain 1
(config-bridge-domain)#interface xe1.1
(config-bridge-domain)#interface xe2.1
(config-bridge-domain)#exit
(config)#commit
```

Creating a Sub-interface with Encapsulation

Configure Single Encapsulation with VLAN Range (dot1q)

Create sub-interface xe1.100 and define a VLAN range (100 to 200) using 802.1Q encapsulation. This enables the interface to handle multiple VLAN-tagged traffic.

```
#configure terminal
(config)#interface xe1.100 switchport
(config-if)#encapsulation dot1q 100-200
(config-if)#exit
```

Configure Single Encapsulation with VLAN Range (dot1ad)

Apply 802.1ad (Q-in-Q) encapsulation to the sub-interface for VLANs 100 to 200, allowing service provider-style tunneling with S-tags.

```
#configure terminal
(config)#interface xe1.100 switchport
(config-if)#encapsulation dot1ad 100-200
(config-if)#exit
```

Configure Double Encapsulation (dot1q)

Set up double VLAN tagging (both outer and inner VLAN 10) on xe1.100 using dot1q encapsulation. This prepares the interface to handle nested VLAN tags.

```
#configure terminal
(config)#interface xe1.100 switchport
(config-if)#encapsulation dot1q 10 inner-dot1q 10
(config-if)#exit
```

Configure Double Encapsulation (dot1ad)

Configure sub-interface xe1.200 with outer tag 20 (dot1ad) and inner tag 20 (dot1q), enabling Q-in-Q double tagging.

```
#configure terminal
(config)#interface xe1.200 switchport
```

```
(config-if)#encapsulation dot1ad 20 inner-dot1q 20
(config-if)#exit
```

Set Default Encapsulation

Assign the default encapsulation type to the interface, which allows any traffic not matched by specific sub-interfaces.

```
#configure terminal
(config)#interface xe1.101 switchport
(config-if)#encapsulation default
(config-if)#exit
```

Set Untagged Encapsulation

Configure the interface to accept untagged traffic. This is typical for access ports connected to hosts or customers.

```
#configure terminal
(config)#interface xe1.102 switchport
(config-if)#encapsulation untagged
(config-if)#exit
```

Rewrite Operations

Apply VLAN Push Rewrite

Configure `xe1.1` to add `VLAN 100` (with TPID `0x8100`) to incoming traffic that matches `VLAN 10`. On `xe2.2`, configure double-tagged encapsulation to match the pushed frame.

```
#configure terminal
(config)#interface xe1.1 switchport
(config-if)#encapsulation dot1q 10
(config-if)#rewrite push 0x8100 100
(config-if)#exit
(config)#interface xe2.2 switchport
(config-if)#encapsulation dot1q 100 inner-dot1q 10
(config-if)#exit
(config)#bridge-domain 1
(config-bridge-domain)#interface xe1.1
(cconfig-bridge-domain)#interface xe2.1
(config-bridge-domain)#exit
```

Note: For incoming traffic at sub-interface “interface IFNAME”, the "rewrite push" will add VLAN as 100 with TPID values 8100.

Note: For outgoing traffic at sub-interface "interface IFNAME", the "rewrite push" will pop the VLAN. The egress pop removes whatever outer VLAN tag is present, regardless of its value. This is not restricted to VLAN 100.

Apply VLAN Translate Rewrite

Set xe1.1 to translate VLAN 200 to 100 using TPID 0x9100. This is useful for interoperability between customer and provider VLAN schemes.

```
#configure terminal
(config)#interface xe1
(config-if)#dot1ad ethertype 0x9100
```

```
(config-if)#interface xe1.1 switchport
(config-if)#encapsulation dot1ad 200
(config-if)#rewrite translate 1-to-1 0x9100 100
(config-if)#interface xe2
(config-if)#dot1ad ethertype 0x9100
(config-if)#interface xe2.2 switchport
(config-if)#encapsulation dot1ad 100
(config-if)#exit
(config)#bridge-domain 1
(config-bridge-domain)#interface xe1.1
(config-bridge-domain)#interface xe2.1
```

Note: For incoming and outgoing traffic at sub-interface “interface IFNAME”, the "rewrite translate" will update VLAN tag with TPID values 9100.

Apply VLAN Pop Rewrite

Configure `xe1.1` to remove the VLAN tag from incoming frames. On `xe2.2`, accept the resulting untagged traffic.

```
#configure terminal
(config)#interface xe1.1 switchport
(config-if)#encapsulation dot1q 100
(config-if)#rewrite pop
(config-if)#interface xe2.2 switchport
(config-if)#encapsulation untagged
(config-if)#exit
(config)#bridge-domain 1
(config-xc)#interface xe1.1
(config-xc)#interface xe2.1
```

Note: For incoming traffic at sub-interface “interface IFNAME”, the "rewrite pop" will pop the VLAN.

Note: For outgoing traffic at sub-interface “interface IFNAME”, the "rewrite pop" will add VLAN tag with TPID values `8100`.

Note: Push, pop, and translate rewrite operations are supported with TPID values `8100/88a8/9100/9200` as symmetric operations.

Remove All Sub-interfaces

Remove all sub-interfaces configured under xe1.

```
#configure terminal
(config)#interface xe1
(config-if)#no subinterfaces
```

Note: The command "no subinterfaces" will remove all the sub-interfaces within a particular interface. OcNOS allows the same physical interface to support both L2 and L3 sub-interfaces.

Validation

```
#show bridge-domain
Bridge Id   interfaces       Status
--------------+---------------+---------------+-------
 1               xe1.1              UP
                  xe2.1              UP
```

1. Command to display the learned MAC entries of bridge domain

```
#show mac address-table dynamic bridge-domain id 1
Bridge  MAC Address     Type      Ports
```

```
    ------+---------------+---------+---------+
  1       0022.3344.5566   dynamic   xe1.1

#show mac address-table dynamic bridge-domain all
Bridge MAC Address     Type      Ports
    ------+---------------+---------+---------+
 1      0022.3344.5566  dynamic   xe1.1

#show mac address-table dynamic bridge-domain interface xe1.1
Bridge MAC Address     Type      Ports
    ------+---------------+---------+---------+
 1      0022.3344.5566  dynamic   xe1.1




#show mac address-table dynamic bridge-domain address 0022.3344.5566
Bridge MAC Address     Type      Ports
    ------+---------------+---------+---------+
 1      0022.3344.5566  dynamic   xe1.1
```

2. Command to clear the learned MAC entries

```
#clear mac address-table dynamic bridge-domain id 1
#clear mac address-table dynamic bridge-domain id 1 interface xe1.1
#clear mac address-table dynamic bridge-domain id 1 address 0022.3344.5566
#clear mac address-table dynamic bridge-domain all


#show mac address-table dynamic bridge-domain id 1
Bridge MAC Address     Type      Ports
    ------+---------------+---------+---------+
```

Configuring Static MAC Address on L2 Sub-interface

In a bridge-domain, static MAC addresses can be configured on specific sub-interfaces to control traffic flow precisely. This setup supports Layer 2 switching between sub-interfaces, whether they reside on the same or different physical ports.

The bridge-domain uses 802.1Q VLAN tagging to identify and separate traffic. Broadcast, unknown Unicast, and Multicast (BUM) traffic is flooded within the bridge-domain, ensuring delivery even in the absence of MAC learning. For known unicast traffic, forwarding decisions are based on the Layer 2 forwarding database (FDB).

When a destination MAC address is statically configured on a sub-interface, all matching traffic will egress only via that sub-interface, eliminating unnecessary flooding. This deterministic forwarding improves efficiency and enhances control over traffic paths.

1. **Configure Physical Interfaces in Switchport Mode:** Enable Layer 2 mode on interfaces xe1, xe2, and xe3 for sub-interface creation.

```
(config)#interface xe1
(config-if)#switchport
(config-if)#exit

(config)#interface xe2
```

```
(config-if)#switchport
(config-if)#exit

(config)#interface xe3
(config-if)#switchport
(config-if)#exit
```

2. **Create Sub-interfaces and Set VLAN Encapsulation:** Configure sub-interfaces xe1.1, xe2.1, and xe3.1 to match VLAN 100 tagged traffic using 802.1Q encapsulation.

```
(config)#interface xe1.1 switchport
(config-if)#encapsulation dot1q 100
(config-if)#exit

(config)#interface xe2.1 switchport
(config-if)#encapsulation dot1q 100
(config-if)#exit

(config)#interface xe3.1 switchport
(config-if)#encapsulation dot1q 100
(config-if)#exit
```

3. **Create Bridge-Domain and Attach Sub-interfaces:** Create bridge-domain 1 and associate all three sub-interfaces, enabling Layer 2 switching between them.

```
(config)#bridge-domain 1
(config-bridge-domain)#interface xe1.1
(config-bridge-domain)#interface xe2.1
(config-bridge-domain)#interface xe3.1
```

4. **Configure Static MAC Entries:** Map MAC 0000.0100.0001 to sub-interface `xe1.1` and MAC `0010.9400.0002` to `xe2.1`. This forces unicast traffic to these MACs to egress only from the specified ports, avoiding flooding.

```
(config-bridge-domain)#mac 0000.0100.0001 forward xe1.1
(config-bridge-domain)#mac 0010.9400.0002 forward xe2.1
(config-bridge-domain)#exit
(config)#commit

end
```

Validation

Confirm that static MAC entries and sub-interfaces are correctly attached to bridge-domain 1.

Verify Running Configuration

```
!
interface xe1
 switchport
!
interface xe1.1 switchport
 encapsulation dot1q 100
!
interface xe2
```

```
 switchport
!
interface xe2.1 switchport
 encapsulation dot1q 100
!
interface xe3
 switchport
!
interface xe3.1 switchport
 encapsulation dot1q 100
!
 exit
!
bridge-domain 1
 interface xe1.1
 interface xe2.1
 interface xe3.1
 mac 0000.0100.0001 forward xe1.1
 mac 0010.9400.0002 forward xe2.1
!
!

#show running-config bridge-domain
!
bridge-domain 1
 interface xe1.1
 interface xe2.1
 interface xe3.1
 mac 0000.0100.0001 forward xe1.1
 mac 0010.9400.0002 forward xe2.1
!
!
```

Monitor Interface Traffic

Observe traffic flow patterns on each sub-interface to validate unicast forwarding based on the static MACs.

```
#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx mbps   |    Rx pps   |    Tx mbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 xe1                 0.00           0             242.13         236450
 xe1.1               0.00           0             241.82         236149
 xe2                 0.00           0             181.24         176993
 xe2.1               0.00           0             181.10         176852
 xe3                 399.78         390406        0.00           0
 xe3.1               397.50         388183        0.00           0
```

Verify Static MAC Address Table

Verify that the static MAC entries are configured correctly and are active in the bridge-domain.

```
#show mac address-table static bridge-domain all

Bridge  MAC Address     Type      Ports

    ------+--------------+---------+---------+

1    0000.0100.0001  static    xe1.1
1    0010.9400.0002  static    xe2.1
```

Static MAC Commands

The following new commands are introduced as part of the static MAC support enhancement; for more details, refer to the Layer 2 Sub-interface Commands section.

- clear mac address-table dynamic bridge-domain
- mac address IFNAME
- show mac address-table bridge-domain

Troubleshooting

MAC not learning: Ensure correct VLAN tags and that sub-interfaces are operational.

Flooding despite known MAC: Check for missing static entries or bridge-domain misconfiguration.

No traffic flow: Use the `show interface counters rate` command to verify Transmit (TX) and Receive (RX) interface activity.

Glossary

The following provides definitions for key terms or abbreviations and their meanings used throughout this document:

Key Terms/Acronym	Description
Bridge-Domain	Logical L2 switch fabric grouping multiple sub-interfaces.
BUM	Broadcast, Unknown Unicast, Multicast traffic.
FDB	Forwarding Database containing learned or static MAC addresses.
Sub-interface	Virtual interface configured with VLAN encapsulation.

CHAPTER 22 Layer 2 Control Protocols Tunneling

Overview

Layer 2 Control Protocol (L2CP) Tunneling is a specialized networking feature that allows specific control frames—like STP, LACP, LLDP, or CDP—to be carried transparently across a service provider's network. Tunneling encapsulates the L2CP frames by changing customer’s reserved MAC address with a unique provider multicast MAC address.

The L2CP tunneling is supported on the IEEE 802.1Q networking for handling L2CP frames whether to forward or peer or discard them in an Ethernet network.

In Provider Bridging (PB), the IEEE 802.1Q provides a mechanism for separating the Layer2 control plane into multiple customer and provider control planes. It allows a certain layer 2 control protocol to operate only within a provider network, or to allow interaction between the customer and the provider network, or to pass transparently through a provider network with complete isolation from other customer networks.

In case of non-Provider Bridging, packet is forwarded without changing any MAC.

The behavior of an L2CP frame is a strict evaluation based on the destination MAC address and the specific service attributes configured on the interface.

When a L2CP frame is received at PE router, the device must choose one of following three paths - Discard, Peer, or Pass/Tunnel.

Discard	The L2CP frame is dropped immediately. It is neither processed by the local switch nor forwarded to any other part of the network.
Peer	The L2CP frame will be processed. When a L2CP frame is Peered, the PE device recognizes the protocol and processes it.
Pass/Tunnel	The Pass action treats the control frame exactly like standard user data. The frame is forwarded transparently across the service provider’s core.

The document describes L2CP tunneling process in various environments such as Provider Bridge (PB), L2VPN.

L2CP Tunneling in Provider Bridging

In a Provider Bridging (PB) environment, L2CP tunneling allows Customer Edge (CE) nodes to exchange control plane traffic transparently across a Service Provider network. This ensures that protocols like STP or LACP remain end-to-end between customer sites rather than being intercepted by the provider.

1. Frame Identification

   In the context of Provider Bridging, L2CP frames are identified by specific Destination MAC (DMAC) addresses. While these are often configurable via the CLI, the common defaults are:

   - 01:00:0C:CD:CD:D0
   - 01:04:DF:CD:CD:D0

2. Ingress Processing (At the CEP Port)

When a control frame arrives at the Customer Edge Port (CEP) of a Provider Edge (PE) bridge, the following transformations occur:

- **MAC Rewrite:** The original multicast DMAC is replaced with a predefined tunneling multicast address: 01-00-C2-CD-CD-D0. This "hides" the control frame from intermediate provider switches.
- **VLAN Tagging**: If the frame is already tagged with a Customer VLAN (C-VLAN) or is untagged, the PE bridge appends the appropriate Service VLAN (S-VLAN) tag.
  - This mapping is determined by the port's registration table or VLAN translation table.
- **Forwarding:** The frame is now treated as a standard data packet and forwarded across the Service Provider network.

3. Egress Processing (At the PNP Port)

   When the tunneled packet reaches the Provider Network Port (PNP) at the remote end, the process is reversed:

- **MAC Restoration:** The tunneling multicast address (01-00-C2-CD-CD-D0) is swapped back to the original protocol-specific multicast address.
- **VLAN Stripping/Update:** The S-VLAN tag is removed or modified, and the C-VLAN is handled according to the egress registration/translation table settings.
- **Delivery**: The original control frame is delivered to the remote CE node in its native format.

The following illustration depicts the L2CP frames flow in a PB tunneling environment.

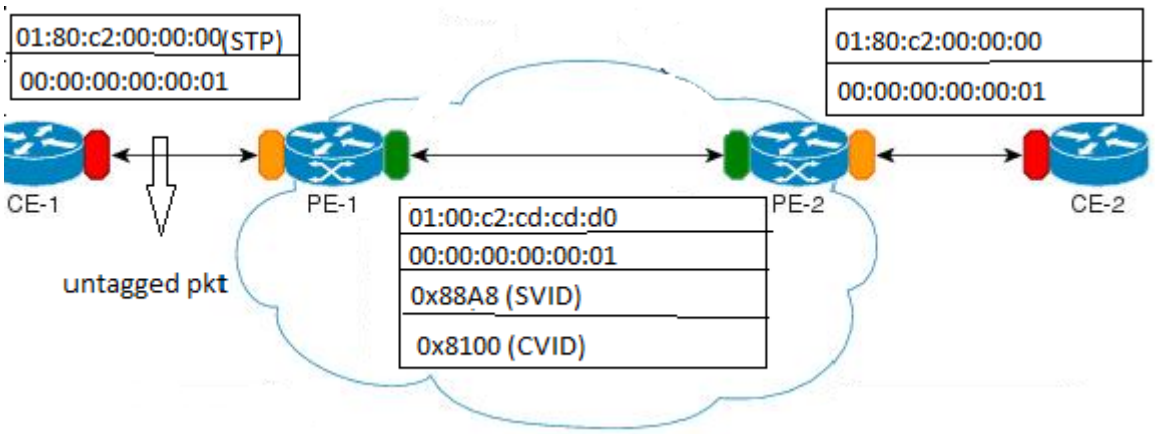


Figure 22-41: L2CP Tunneling Process in Provider Bridge

Default Behavior

When a control packet arrives at a Provider Edge (PE) router on an Attachment Circuit (AC) port, the system treats it as standard customer traffic.

- Encapsulation: The PE router takes the incoming control frame (tagged or untagged) and encapsulates it directly with MPLS labels (the Transport label and the Service/VC label).
- Transport: The packet is switched across the MPLS core like any other data packet. The provider's core routers (P-routers) do not "see" the control MAC addresses because they are hidden behind MPLS headers.
- Decapsulation: The remote PE router strips the MPLS labels and forwards the original L2CP frame to the destination CE.

The LACP Exception: By default, LACP frames are often consumed (peered) by the PE to manage the local link aggregation between the CE and PE. All other L2CP protocols are typically tunneled by default.

L2CP Behavior

Default L2CP decision in provider bridging case:

Table 22-2: Default L2CP decision for Provider Bridging

Protocol Type	L2CP destination address	Ethertype/subtype	Default L2CP action
STP (Spanning Tree Protocols)	01-80-c2-00-00-00	N/A	PEER
LACP (Link Aggregation Control Protocol)	01-80-c2-00-00-02	ethertype 0x8809 and subtype 0x1 or 0x2	PEER
DOT1X (Port Authentication (802.1 X))	01-80-c2-00-00-03	N/A	PEER
LLDP (Link layer discovery protocol)	01-80-c2-00-00-0e	ethertype 0x88CC	PEER
EFM (Ethernet first mile (Link OAM))	01-80-c2-00-00-02	ethertype 0x8809 and subtype 0x3	PEER
ELMI (Ethernet Local Management Interface)	01-80-c2-00-00-07	ethertype 0x88EE	PEER

L2CP Configuration in Provider Bridging

Enabling tunneling at interface:

```
(config)#bridge 1 protocol provider-rstp edge
(config)#vlan database
(config-vlan)#vlan 2-10 bridge 1 state enable
(config-vlan)#vlan 11 type service point-point bridge 1 state enable
(config-vlan)#ex
(config)#cvlan registration table map1 bridge 1
(config-cvlan-registration)#cvlan 2 svlan 11
(config-cvlan-registration)#ex
(config)#interface xe1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode customer-edge hybrid
(config-if)#switchport customer-edge hybrid allowed vlan all
(config-if)#switchport customer-edge vlan registration map1
(config-if)#l2protocol stp tunnel
#show running-config interface xe1
!
 interface xe1
 speed 1g
 switchport
 bridge-group 1
 switchport mode customer-edge hybrid
 switchport customer-edge hybrid allowed vlan all
 switchport customer-edge vlan registration map1
 l2protocol stp tunnel
 customer-spanning-tree provider-edge svlan 11 path-cost 128
(config-if)#commit
```

Configuring egress interfaces:

```
(config)#interface xe2
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode provider-network
(config-if)#switchport provider-network allowed vlan all
(config-if)#commit
```

Validation

To display L2protocol information:

```
#show l2protocol processing interface xe1
Bridge   Interface Name  Protocol     Processing Status     Hardware Status
======   ==============  ========     =================     ===============
1        xe1             stp          Tunnel                Tunnel
1        xe1             lacp         Peer                  Peer
1        xe1             dot1x        Peer                  Peer
1        xe1             lldp         Peer                  Peer
1        xe1             efm          Peer                  Peer
1        xe1             elmi         Peer                  Peer
```

To display L2protocol counters:

```
#show l2protocol interface counters
Interface xe1
Tunnel               :  stp                 : 45
```

L2CP Tunneling in L2VPN (VPLS/VPWS/Hybrid)

In L2VPN environments—such as VPLS (Multipoint) or VPWS (Point-to-Point) or Hybrid (Bridge+L2VPN)—L2CP tunneling ensures that Layer 2 control protocols (like STP, LLDP, or CDP) can traverse the MPLS core. This allows geographically separated Customer Edge (CE) devices to behave as if they are on the same local segment.

Default Behavior

A Hybrid Port is a complex interface that handles both local Layer 2 switching (Bridge) and L2VPN (VPLS/VPWS) services simultaneously.

The Switch to Peering: Unlike standard AC ports, when a port is configured as Hybrid, the default behavior for L2CP often shifts to Peering mode. In this mode, the PE router "intercepts" and processes the control frames itself (e.g., the PE participates in the customer's Spanning Tree).

Overriding Behavior: If the goal is to pass these frames through to the remote site instead of processing them locally, you must manually apply L2CP override configurations (such as l2-protocol tunneling commands) to force the hybrid port back into a tunneling state for specific protocols.

The following illustration depicts the L2CP frames tunneling in a L2VPN environment.

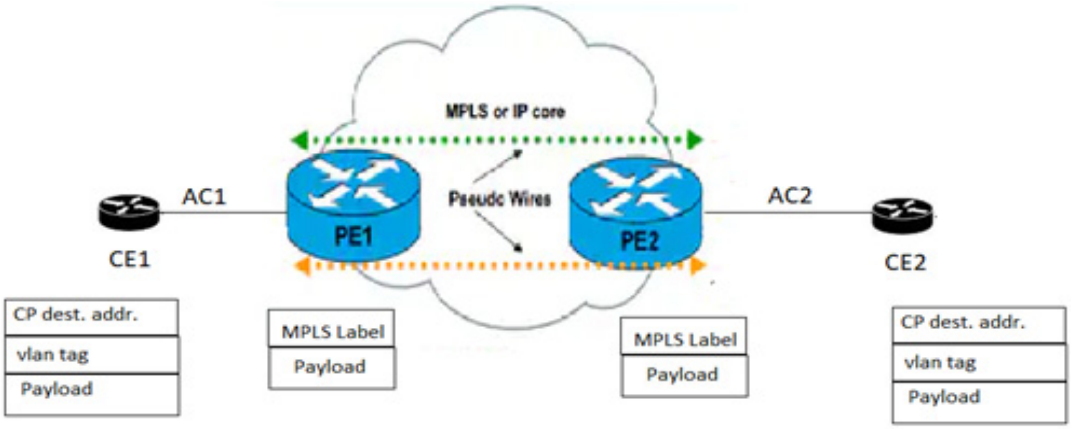


Figure 22-42: L2CP tunneling in L2VPN

L2CP Behavior

Default L2CP behavior in VPLS/VPWS/Hybrid environments:

VPLS/VPWS

Table 22-3: Default L2CP decision for VPLS/VPWS

Protocol Type	L2CP destination address	Default L2CP action
STP (Spanning Tree Protocols)	01-80-c2-00-00-00	TUNEEL
LACP (Link Aggregation Control Protocol)	01-80-c2-00-00-02	PEER
DOT1X (Port Authentication (802.1 X))	01-80-c2-00-00-03	TUNNEL
LLDP (Link layer discovery protocol)	01-80-c2-00-00-0e	TUNNEL
EFM (Ethernet first mile (Link OAM))	01-80-c2-00-00-02	TUNNEL
ELMI (Ethernet Local Management Interface)	01-80-c2-00-00-07	TUNNEL

Hybrid (Bridge+ L2VPN):

Table 22-4: Default L2CP decision for Hsybrid

Protocol Type	L2CP destination address	Default L2CP action
STP (Spanning Tree Protocols)	01-80-c2-00-00-00	PEER
LACP (Link Aggregation Control Protocol)	01-80-c2-00-00-02	PEER
DOT1X (Port Authentication (802.1 X))	01-80-c2-00-00-03	PEER
LLDP (Link layer discovery protocol)	01-80-c2-00-00-0e	PEER
EFM (Ethernet first mile (Link OAM))	01-80-c2-00-00-02	PEER
ELMI (Ethernet Local Management Interface)	01-80-c2-00-00-07	PEER

Basic Configuration for L2CP in VPLS

Enabling tunneling at ingress VPLS interface:

```
#show run in xe12
!
interface xe12
 speed 1g
 mpls-l2-circuit vc1 service-template svc1
!
#config ter
#(config)interface xe12
(config-if)#commit
```

Validation

To display L2CP information:

```
#show l2protocol processing interface xe12

Bridge   Interface Name  Protocol     Processing Status     Hardware Status
======   ==============  ========     =================     ===============
-        xe12             stp          Discard               Discard
-        xe12             lacp         None                  Peer
-        xe12             dot1x        None                  Tunnel
-        xe12             lldp         None                  Tunnel
-        xe12             efm          None                  Tunnel
-        xe12             elmi         None                  Tunnel
```

L2CP Configuration in Hybrid + VPLS

Enabling tunneling at bridged interface:

```
(config-if)#show run in xe11
!
```

```
interface xe11
 speed 1g
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 mpls-l2-circuit vc1 service-template svc1

#config ter
#(config)interface xe11
(config-if)#l2protocol stp tunnel
(config-if)#commit
(config-if)#end
```

Validation

To display L2CP information:

```
#show l2protocol processing interface xe11
Bridge   Interface Name  Protocol     Processing Status     Hardware Status
======   ==============  ========     =================     ===============
-        xe11             stp          Tunnel                Tunnel
-        xe11             lacp         None                  Peer
-        xe11             dot1x        None                  Peer
-        xe11             lldp         None                  Peer
-        xe11             efm          None                  Peer
-        xe11             elmi         None                  Peer

(config)#in xe11
(config-if)#no l2protocol stp
(config-if)#end
#show l2protocol processing interface xe11
Bridge   Interface Name  Protocol     Processing Status     Hardware Status
======   ==============  ========     =================     ===============
-        xe11             stp          None                  Peer
-        xe11             lacp         None                  Peer
-        xe11             dot1x        None                  Peer
-        xe11             lldp         None                  Peer
-        xe11             efm          None                  Peer
-        xe11             elmi         None                  Peer
```

Note: If the configuration is not done, hardware status shows the default values while the configured will be none. On configuring L2CP on interface, configured and hardware status will be same.

L2CP Tunneling for EVPN MPLS

EVPN-MPLS utilizes the Border Gateway Protocol (BGP) as a control plane to distribute MAC addresses and reachability information, while using an MPLS data plane for transport. In this architecture, L2CP tunneling is essential for providing a "transparent wire" experience between Customer Edge (CE) devices across a Layer 3 MPLS core.

The following illustration depicts the L2CP frames tunneling in an EVPN MPLS Single Home environment.

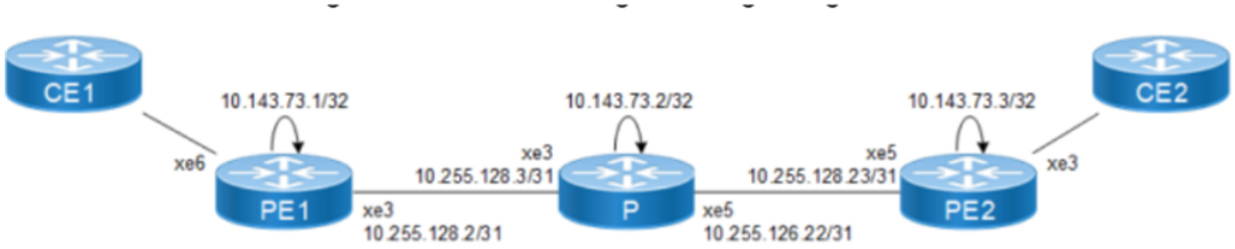


Figure 22-43: L2CP tunneling in EVPN MPLS SH

Default Behavior

EVPN-MPLS handles L2CP tunneling through a Sub-interface (Sub-ifp) framework. While the actual transport happens over the EVPN instance, the policy—determining which protocols are tunneled—is typically defined at the Parent Interface level (the physical port or LAG connecting the CE).

Because the MPLS core operates at Layer 3, it is naturally unaware of the Ethernet headers or Layer-2 control protocols, ensuring strict separation between the provider network and customer Layer-2 domains. This separation ensures that the provider's core routers (P-routers) are never burdened by customer’s network changes.

L2CP tunneling in EVPN-MPLS enables L2CP frames to be transparently transported between CE devices across both single-homed and multi-homed Ethernet segments. L2CP frames are identified at the ingress PE based on well-known destination MAC addresses, Ethertype values, and configured service policies, which determine whether the frames are tunneled, locally processed, or discarded.

L2CP Behavior

When an L2CP frame is tunneled, the ingress PE suppresses local protocol processing and encapsulates the complete Ethernet frame into EVPN and MPLS headers before forwarding it across the MPLS core. The frame is treated as a standard data packet. Core routers perform label switching only and remain unaware of the control protocol semantics. At the egress PE removes the EVPN and MPLS encapsulation and delivers the original L2CP frame unchanged to the destination CE device. This mechanism preserves end-to-end Layer-2 control plane behavior for customer networks while maintaining isolation and scalability within the EVPN-MPLS provider infrastructure.

- Tunnel - Transparently tunnels the L2 control plane BPDU such as Dot1x, EFM, ELMI,LLDP, xSTP, LACP across EVPN-MPLS networks based on configured egress tunnels.
- Peer - Uplifts the L2 control packet to the CPU/control plane for processing.
- Discard - Drops the L2 control packers .

Default behavior is Peer.

One of the unique strengths of EVPN-MPLS is Multi-homing (All-Active or Single-Active). When L2CP frames are tunneled in a multi-homed environment, the EVPN control plane ensures that frames like STP BPDUs are handled correctly to avoid loops, often using Ethernet Segment Identifiers (ESI) to manage split-horizon forwarding.

The following illustration depicts the L2CP frames tunneling in an EVPN MPLS Multi Home environment.

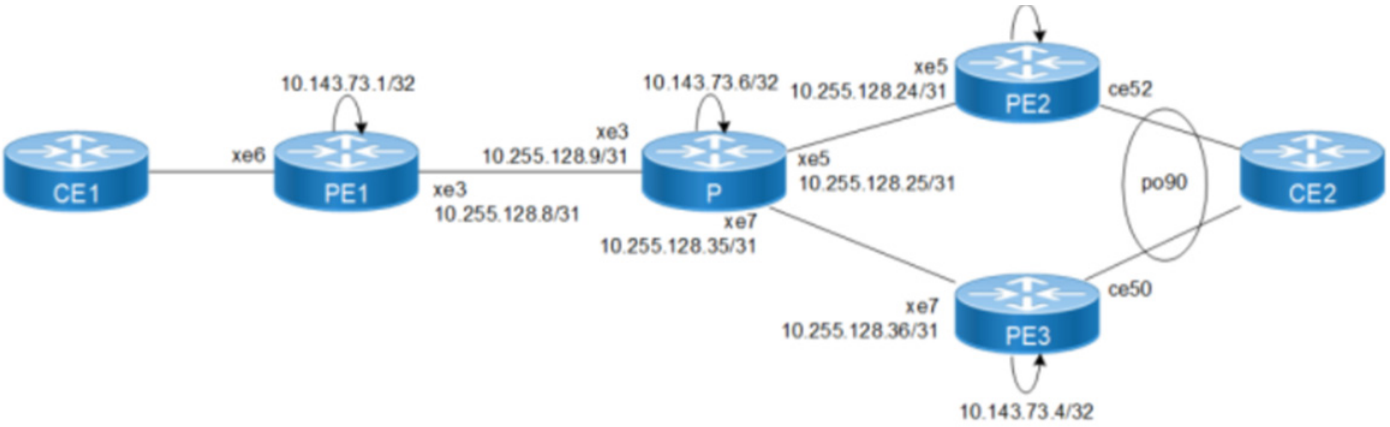


Figure 22-44: L2CP tunneling for EVPN MPLS MH

Basic Configuration for L2CP in EVPN MPLS

`(config)#in xe6`	Entering into interface level of access side interface
`(config-if)#l2protocol <protocol> tunnel`	Enabling tunnel for the L2CP protocol
`(config-if)#l2protocol <protocol> peer`	Enabling peer for the L2CP protocol
`(config-if)#l2protocol <protocol> discard`	Enabling discard for the L2CP protocol

Validation

```
PE1#show l2protocol processing interface <interface>
 Bridge    Interface Name   Protocol      Processing Status      Hardware Status
 ======    ==============   ========      =================      ===============
 -         xe6              stp           Tunnel                   Peer
 -         xe6              lacp          Tunnel                   Peer
 -         xe6              dot1x         Peer                     Peer
 -         xe6              lldp          Peer                     Peer
 -         xe6              efm           Discard                  Discard
 -         xe6              elmi          Discard                  Discard
 -         xe6              synce         Discard                  Discard

PE1#show l2protocol interface po90 counters
 Interface po90
 Peer                 :  lacp                 : 94
 Peer                 :  stp                  : 298
 Peer                 :  elmi                 : 172
 Peer                 :  dot1x                : 172
 Discard              :  stp                  : 6558
 Discard              :  elmi                 : 8326
 Discard              :  dot1x                : 9839
Tunnel counters won't get incremented as per design.
```

```
PE1#show interface counters queue-stats
 E - Egress, I - Ingress, Q-Size is in bytes
  * indicates monitor is active
```

Interface	Queue/Class-map	Q-Size	Tx pkts	Tx bytes	Dropped pkts	Dropped bytes
cpu	reserved-mc	(E) 2097152	6	522	0	0
cpu	bgp	(E) 1048576	2	145	0	0
cpu	rsvp-ldp	(E) 1048576	7	1060	0	0
cpu	bpdu	(E) 1048576	6481	4830520	0	0
ge6	q0	(E) 1253376	350	258691	0	0
ge6	q6	(E) 1253376	114	10338	0	0
ge7	q0	(E) 1253376	6	2708	0	0
ge7	q6	(E) 1253376	2	186	0	0
ge8	q0	(E) 1253376	5177	3859861	0	0
xe12	q6	(E) 12517376	6	517	0	0
xe15	q0	(E) 12517376	2	1281	0	0
xe16	q0	(E) 12517376	2253	1694682	0	0

L2CP Tunneling in VXLAN

L2CP tunneling provides support for tunneling control plane frames across VxLAN/MH.

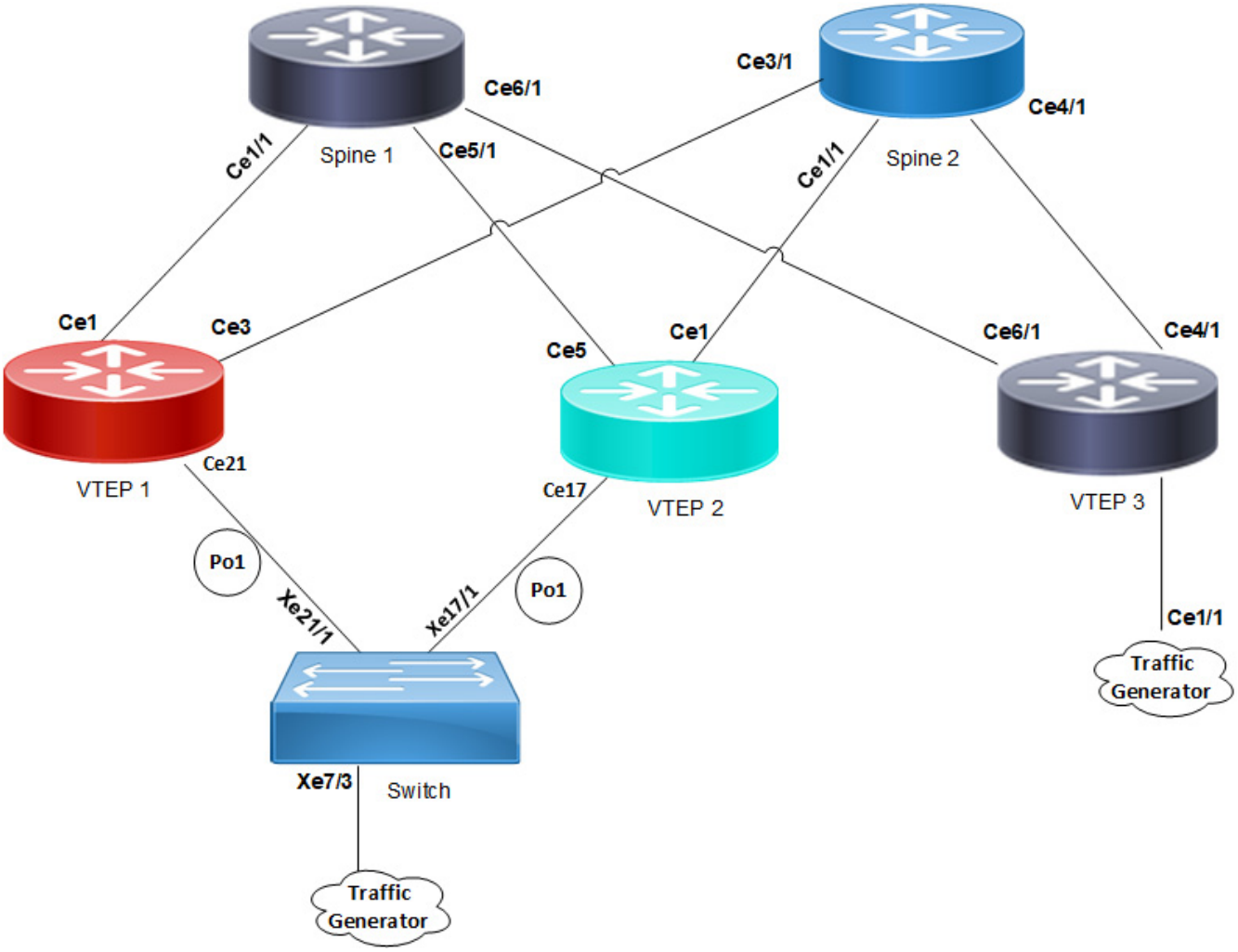


Figure 22-45: L2CP tunneling in VXLAN

VxLAN creates LAN segments using a MAC in IP encapsulation. The encapsulation carries the original L2 frame received from a host to the destination in another server using IP tunnels. The endpoints of the virtualized tunnel formed using VxLAN are called VTEPs (VXLAN Tunnel EndPoints).

L2CP tunneling provides support for tunneling control plane frames across VxLAN with MH/SH combination.

Any L2CP frame that is destined towards other end with a multicast destination MAC Address for L2 protocol is decided by looking at the frame and upon the configured values of the L2CP service attributes.

As and when control packets with default destination MAC address for any L2 protocol is generated, it will be forwarded by VTEPs that are part of MH towards the VTEP that is part of SH and vice versa.

During this operation, the default destination MAC address for any L2 protocol is replaced with predefined multicast address as destination for tunneling the packets across spine nodes. When tunneled control packet with pre-defined multicast address received on ingress port on the other end of the VTEP, the multicast address is replaced with corresponding control packet multicast address.

L2CP Tunneling Actions in Different Networks

Table 22-5: Summary of L2CP Tunneling Actions

Environment	Primary Transport Method	Ingress Action (Transformation)	Egress Action (Restoration)	Default L2CP Behavior	Key Identification
Provider Bridging (802.1ad / QinQ)	MAC Rewrite + S-Tag	Replaces DMAC with Tunnel MAC (e.g., 01-00-C2-CD-CD-D0) and adds S-VLAN tag.	Restores original Control DMAC and removes S-VLAN tag.	Discard/Peer (Depends on vendor)	Multicast DMAC & C-VLAN
L2VPN (VPLS / VPWS)	MPLS Label Stack	Encapsulates the entire L2 frame into MPLS Service/Transport labels.	Strips MPLS labels to reveal the original Ethernet frame.	Tunnel (Except LACP)	AC Port Association
EVPN-MPLS	BGP Control Plane + MPLS Data Plane	Encapsulates frame into EVPN/MPLS headers; suppresses local CPU processing.	Strips EVPN/MPLS labels and forwards original frame to CE.	Peer	Parent Interface Policy / DMAC
Hybrid Port (Bridge+L2VPN)	Mixed Switching Logic	Context-dependent; can act as a local Bridge (Peer) or a Pipe (Tunnel).	Depends on whether the frame was switched locally or tunneled.	Peer	Sub-interface Config

CHAPTER 23 ErrDisable for Link-Flapping Configuration

If a link flaps continuously, the interface goes into ErrDisable state. When a port is the ErrDisable state, it is effectively shut down and no traffic is sent or received on that port. The port can be recovered from the ErrDisable state manually (shutting down the interface) or automatically (setting a timeout value).

Note:

- An interface should change state as up-down to complete one cycle of a link flap.
- Admin shut/no-shut is considered as a link-flap for errdisable.
- The LED does not glow when an interface is in the errdisable state.
- Errdisable is supported only on physical interfaces.
- A LAG interface does not go into the errdisable state when all of its member ports are in the errdisable state
- The error disable computation is based on a sliding window of time. The window size is configurable in seconds. This window is taken as the current time to the last <t> second, where <t> is the configured window size. If the accumulated link flap count reaches the maximum flap count for a particular sliding window, a link flap error disable fault is triggered.

Topology

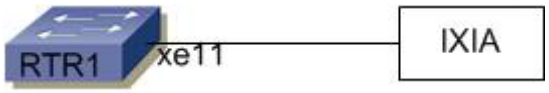


Figure 23-46: ErrDisable

Automatic Recovery

By default, an interface goes into the ErrDisable state when a link flaps 5 times in 10 seconds. An interface is recovered from the ErrDisable state when the configured non-zero errdisable time-out interval value expires.

RTR1

`#configure terminal`	Enter configure mode.
`(config)#errdisable cause link-flap`	Enable ErrDisable due to link-flap
`(config)#errdisable link-flap-setting max-flaps 2 time 30`	Configure Link flap settings. Max link flap count and interval for linkFlap Timer
`(config)#errdisable timeout interval 50`	Configure interval to recover from error disable state
`(config)#commit`	Commit the candidate configuration to the running configuration.
`(config)#exit`	Exit interface mode

Note: Automatic recovery timeout is disabled, if you configure `errdisable timeout interval 0`

Validation

```
#show errdisable details
```

```
 Error Disable Recovery Timeout Interval : 50 secs
 Link Flap Timer Interval : 30 secs
 Link Flaps allowed Max. count : 2

ErrDisable Cause     Status
---------------      ------
Link-Flap            Enabled
Lag-Mismatch         Disabled
Stp-Bpdu-Guard       Enabled
Mac-move-limit       Disabled
```

Note: Stp-Bpdu-Guard is enabled by default on the global level configuration.

```
#show interface errdisable status
Interfaces that will be enabled at the next timeout
Interface    ErrDisable Cause   Time left(secs)
---------    ----------------   ---------------
xe11         link-flap          38

#show interface brief | include ED
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
xe11       ETH   --    --                down    ED      10g   --       No  No
#
```

Note: Interface xe11 went into the ErrDisable state after flapping 2 times in 30 seconds.

Log Message

`Edge1-SiteX#configure terminal`	Enter configure mode.
`Edge1-SiteX(config)#logging level nsm 4`	Enable Operational log to display recovery message
`Edge1-SiteX(config)#commit`	Commit the candidate configuration to the running configuration.
`Edge1-SiteX(config)#exit`	Exit interface mode

```
2017 Sep 18 11:52:12 : NSM : CRITI : [IFMGR_IF_DOWN_2]: Interface xe11 changed state to
down
(config-if)#no shut
(config-if)#2017 Sep 18 11:52:15 : NSM : CRITI : [IFMGR_IF_UP_2]: Interface xe11 changed
state to up
2017 Sep 18 11:52:15 : NSM : WARN : [VXLAN_OPR_ACCESSPORT_UP_4]: VXLAN Access port on
xe11 is up
2017 Sep 18 11:52:15 : NSM : CRITI : [IFMGR_ERR_DISABLE_DOWN_2]: Interface xe11 moved to
errdisable state due to link-flap
2017 Sep 18 11:52:15 : NSM : CRITI : [IFMGR_IF_DOWN_2]: Interface xe11 changed state to
down
```

Note: Interface xe11 recovered from the ErrDisable state after a 50 second time-out.

Manual Recovery

An interface can be recovered manually from the Errdisable state, when configure shutdown followed by no shutdown using CLI. Shutdown will recover the interface from errdisable state and No shutdown will make the interface up state.

RTR1

`#configure terminal`	Enter configure mode.
`(config)#errdisable cause link-flap`	Enable errdisable due to link-flap
`(config)#errdisable link-flap-setting max-flaps 3 time 20`	Configure Link flap settings. Max link flap count and interval for linkFlap Timer
`(config)#commit`	Commit the candidate configuration to the running configuration.
`(config)#exit`	Exit interface mode

```
#show running-config | include errdisable
errdisable cause link-flap
errdisable link-flap-setting max-flaps 3 time 20
errdisable cause stp-bpdu-guard

#show errdisable details

 Link Flap Timer Interval : 20 secs
 Link Flaps allowed Max. count : 3

ErrDisable Cause     Status
----------------     ------
Link-Flap            Enabled
Lag-Mismatch         Disabled
Stp-Bpdu-Guard       Disabled
Mac-move-limit       Disabled
```

Note: Interface xe11 went into the ErrDisable state after flapping 3 times in 20 seconds.

```
(config)#do show interface errdisable status
Interfaces that will be enabled at the next timeout
Interface    ErrDisable Cause   Time left(secs)
---------    ----------------   ---------------
xe11         link-flap          NA
(config)#do show int brief | include ED
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
xe11       ETH   --    --                down    ED      10g   --       No  No
```

Note: Interface xe11 recovered from the ErrDisable state after entering `shutdown` followed by `no shutdown`.

```
(config)#interface xe11
(config-if)#shutdown
2017 Sep 18 13:02:20 : NSM : WARN : [IFMGR_ERR_DISABLE_UP_4]: Interface xe11 recovered
from link-flap errdisable
(config-if)#no shut
(config-if)#2017 Sep 18 13:02:21 : NSM : CRITI : [IFMGR_IF_UP_2]: Interface xe11 changed
state to up
2017 Sep 18 13:02:21 : NSM : WARN : [VXLAN_OPR_ACCESSPORT_UP_4]: VXLAN Access port on
xe11 is up

config)#do show interface errdisable
(config)#do show interface brief | include ED
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
(config)#
```

If you configure `no errdisable cause link-flap`, at the global level, it recovers all the interfaces from the ErrDisable state

Errdisable at the Interface Level

If you enable errdisable globally, by default all physical interfaces enable link-flap errdisable. To turn off errdisable for an interface, configure the commands below.

`#configure terminal`	Enter configure mode.
`(config)#interface xe11`	Enter into interface level
`(config-if)#no link-flap errdisable`	Disable link-flap errdisable for interface
`(config)#commit`	Commit the candidate configuration to the running configuration.
`(config)#exit`	Exit interface mode

Note: If you configure “no link-flap errdisable” in interface level, either it won’t allow the interface move to errdisable state or it will recover interface from errdisable state

Validation

```
#show run int xe11
!
interface xe11
 description *1/2 member of PO3 - Connected to IXIA 6/6*
 channel-group 3 mode active
 no link-flap errdisable
!
```

CHAPTER 24 Unidirectional Link Detection Configuration

This chapter shows a complete configuration to enable UDLD in a simple network topology.

The purpose of Unidirectional Link Detection protocol (UDLD) is to monitor the physical links and detect when a unidirectional link exists. Upon detection user can either block the port or notify the link status based on the network administrator's configuration.

UDLD works in two different modes:

- Normal mode
- Aggressive mode

Topology

Figure 24-47 shows the topology of the UDLD configuration.

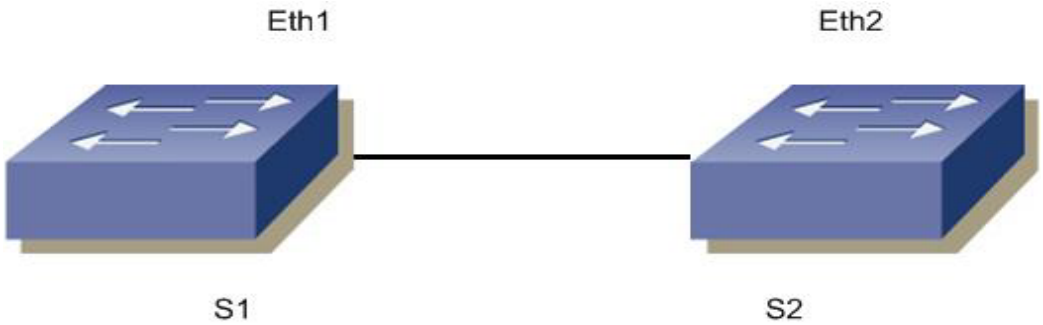


Figure 24-47: UDLD Configuration

S1

`#configure terminal`	Enter configure mode
`(config)#udld enable`	Enable UDLD globally
`(config)# udld message-time 7`	Configure message time for UDLD packets
`(config)#interface eth1`	Enter interface mode
`(config-if)#switchport`	Configure the interface as switch port
`(config-if)#udld state enable`	Enable UDLD on the interface
`(config-if)udld mode normal`	Configure udld mode as normal or aggressive
`(config-if)#commit`	Commit config.
`(config-if)#exit`	Exit from the interface mode

S2

`#configure terminal`	Enter configure mode.
`(config)#udld enable`	Enable UDLD globally.
`(config)#udld message-time 7`	Configure message time for UDLD packets
`(config)#interface eth2`	Enter interface mode
`(config-if)#switchport`	Configure the interface as switch port.
`(config-if)#udld state enable`	Enable UDLD on the interface.
`(config-if)udld mode normal`	Configure udld mode as normal or aggressive
`(config-if)#commit`	Commit config.
`(config-if)#exit`	Exit from the interface mode

Validation

```
#show udld
UDLD: Enable
Message Interval(sec) : 7

Port   UDLD Status      Mode      Link-Status
-----------------------------------------------
Eth1   Enable           Normal    Bi-directional
Eth2   Disable          Normal    Unknown
Eth3   Disable          Normal    Unknown
Eth4   Disable          Normal    Unknown
Eth5   Disable          Normal    Unknown
Eth6   Disable          Normal    Unknown
```

Once the links is made Uni-directional, the output of the command Show udld is as follows:

```
#show udld
UDLD: Enable
Message Interval(sec) : 7

Port   UDLD Status      Mode       Link-Status
-----------------------------------------------
Eth1   Enable           Normal     Unidirectional
Eth2   Disable          Normal     Unknown
Eth3   Disable          Normal     Unknown
Eth4   Disable          Normal     Unknown
Eth5   Disable          Normal     Unknown
Eth6   Disable          Normal     Unknown
```

```
#sh running-config
udld Enable
udld message-time 7

#sh running-config in eth1
!
interface eth1
 switchport
 udld state Enable
!

#sh udld interface eth1
UDLD Status           : Enable
UDLD Mode             : Normal
Link-State            : Unknown
```

For aggressive mode, udld output is as follows:

```
#show udld
    UDLD  : Enable
    Message Interval(sec) : 7


Port   UDLD Status     Mode        Link-Status
-----------------------------------------------
eth1   Enable          Aggressive  Bi-Directional


#sh running config
udld Enable
udld message-time 7

#sh running-config in eth1
  interface eth1
switchport
```

Enable UDLD under bridge-group

S1

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol rstp`	Bridge 1 config
`(config)#udld enable`	Enable UDLD globally
`(config)#udld message-time 7`	Configure message time for UDLD packets
`(config)#commit`	Commit config.
`(config)#interface eth1`	Enter interface mode
`(config-if)#switchport`	Configure the interface as switch port
`(config-if)#bridge-group 1`	Bridge group 1
`(config-if)#udld state enable`	Enable UDLD on the interface
`(config-if)#udld mode normal`	Configure udld mode as normal or aggressive
`(config-if)#commit`	Commit config.
`(config-if)#exit`	Exit from the interface mode

S2

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol rstp`	Bridge 1 config.
`(config)#udld enable`	Enable UDLD globally.
`(config)#udld message-time 7`	Configure message time for UDLD packets
`(config)#commit`	Commit config.
`(config)#interface eth2`	Enter interface mode
`(config-if)#switchport`	Configure the interface as switch port.
`(config-if)#bridge-group 1`	Bridge group 1
`(config-if)#udld state enable`	Enable UDLD on the interface.
`(config-if)#udld mode normal`	Configure udld mode as normal or aggressive
`(config-if)#commit`	Commit config.
`(config-if)#exit`	Exit from the interface mode

Validation

```
#sh running-config | i bridge 1
bridge 1 protocol rstp

#sh running-config in eth1
 interface eth1
 switchport
 bridge-group 1
 udld state Enable
```

```
#sh udld
UDLD                    : Enable
Message Interval(sec)   : 15

Port    UDLD Status     Mode            Link-Status
------------------------------------------------
eth1     Enable          Normal      Bi-Directional
```

CHAPTER 25 MAC Authentication Bypass

MAC Authentication Bypass (MAB) is used for a non-authenticating device (a device without an 802.1X supplicant running on it) connecting to a network with 802.1X enabled. Since there is no supplicant to answer the EAP identity requests from the authenticator (switch, wireless controller, etc.) the authenticator will generate the authentication request for the endpoint using the endpoint's MAC address as the username/password for the Access-Request message.

Note: Multicast address is not accepted for host address of radius-server.

Topology

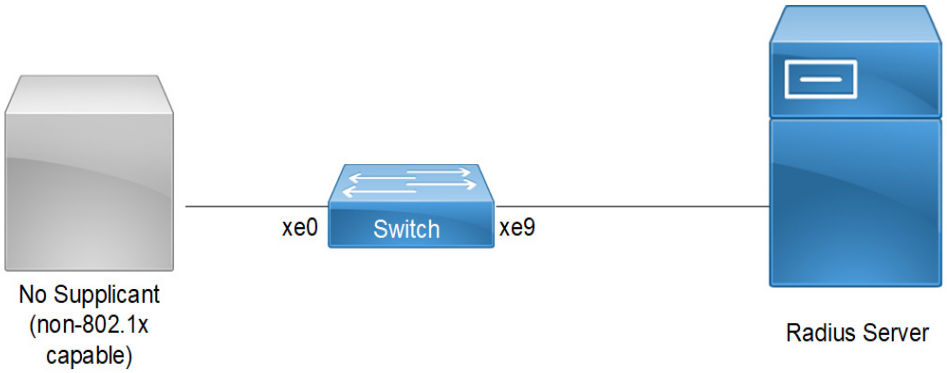


Figure 25-48: MAB Topology

Configuration

Switch Configuration for MAC Authentication Bypass (MAB)

`Switch#configure terminal`	Enter configure mode
`Switch(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1
`OcNOS(config)#commit`	Commit candidate configuration to be running configuration
`Switch(config)#port-security disable`	Disable port security
`Switch(config)#dot1x system-auth-ctrl`	Enable dot1x authentication globally
`Switch(config)#auth-mac system-auth-ctrl`	Enable MAC authentication bypass globally
`Switch(config)#radius-server dot1x host 10.1.1.1 key 0 testing123`	Specify the host IP and key with string name between radius server and client.
`Switch(config)#commit`	Commit transaction
`Switch(config)#interface xe0`	Configure interface xe0
`Switch(config-if)#switchport`	Enable switch port on interface.
`Switch(config-if)#bridge-group 1`	Associate bridge to an interface.
`Switch(config-if)#switchport mode access`	Configure port as access
`Switch(config-if)#dot1x port-control auto`	Enable authentication (via Radius) on port (xe0)
`Switch(config-if)#dot1x mac-auth-bypass enable`	Enable MAC authentication bypass on interface

OcNOS(config)#commit	Commit candidate configuration to be running configuration
Switch(config)#interface xe9	Configure interface xe9
Switch(config-if)#ip address 10.1.1.2/24	Set the IP address on interface xe9
Switch(config-if)#commit	Commit transaction
Switch(config-if)#end	Exit config mode.

Validation

Verify MAB on Switch

```
Switch#show mab all
Global MAC Authentication Enabled
  RADIUS server address: 10.1.1.1:1812
  Next radius message id: 4
  RADIUS client address: not configured

MAB info for interface xe0
  Dot1x timer: Expired
  MAB Authentication Enabled
  Supplicant name: 00:07:E9:A5:3D:FA
  Status: MAC Authorized
  Last rejected MAC:
```

Configuration

MAC Authentication Configuration

Switch#configure terminal	Enter configure mode
Switch(config)#bridge 1 protocol ieee vlan-bridge	Create bridge 1
Switch(config)#port-security disable	Disable port security
Switch(config)#dot1x system-auth-ctrl	Enable dot1x authentication globally
Switch(config)#auth-mac system-auth-ctrl	Enable MAC authentication bypass globally
Switch(config)#radius-server dot1x host 10.1.1.1 key 0 testing123	Specify the host IP and key with string name between radius server and client.
Switch(config)#commit	Commit transaction
Switch(config)#interface xe0	Configure interface xe0
Switch(config-if)#switchport	Enable switch port on interface.
Switch(config-if)#bridge-group 1	Associate bridge to an interface.
Switch(config-if)#switchport mode access	Configure port as access
Switch(config-if)#auth-mac enable	Enable MAC authentication on interface
OcNOS(config)#commit	Commit candidate configuration to be running configuration
Switch(config)#interface xe9	Configure interface xe9
Switch(config-if)#ip address 10.1.1.2/24	Set the IP address on interface xe9

`Switch(config-if)#commit`	Commit transaction
`Switch(config-if)#end`	Exit config mode.

Note: When AUTH-MAC is enabled on the interface MAC-AUTH bypass cannot be enabled and vice-versa.

Validation

Verify MAB on Switch

```
Switch#show mab all
Global MAC Authentication Enabled
  RADIUS server address: 10.1.1.1:1812
  Next radius message id: 9
  RADIUS client address: not configured

MAB info for interface xe0
  Dot1x timer: Expired
  MAB Authentication Disabled
  Supplicant name: 00:07:E9:A5:3D:FA
  Status: MAC Authorized
  Last rejected MAC: 00:07:E9:A5:4E:25
```

CHAPTER 26 Traffic Segmentation-Protected Port

The protected port is a feature that does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port. However, a protected port can communicate with an unprotected port and vice-versa.

The protected port is a feature that does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port. However, a protected port can communicate with an unprotected port and vice-versa.

- Protected port(isolated) to protected port(isolated) - communication is not allowed.
- Protected port(isolated) to protected port(community) - communication is not allowed.
- Protected port(isolated) to protected port(promiscuous) - communication is allowed.
- Protected port(community) to protected port(community) - communication is allowed.
- Protected port(community) to protected port(promiscuous) - communication is allowed.
- Protected port(promiscuous) to protected port(promiscuous) - communication is allowed.
- Unprotected port to protected port(any type) - communication is allowed.

The protected port configuration is local to the switch. This information is not propagated outside the switch. Protected ports across switches can still be able to communicate with each other.

The use of protected ports ensures that there is no exchange of unicast, broadcast, or multicast data traffic between ports on the same switch so that one neighbor does not see the traffic generated by another neighbor.

Topology

Figure 26-49 displays Traffic Segmentation-Protected Port Topology

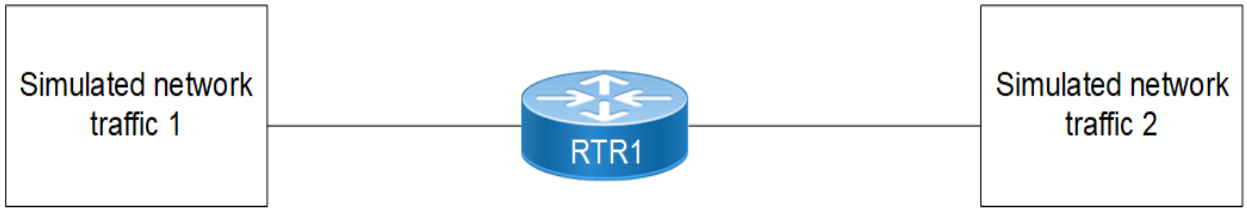


Figure 26-49: Traffic Segmentation-Protected Port Topology

Isolated-Promiscuous Configuration

RTR1

Bridge Configuration:

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure bridge

VLAN Configuration:

`#configure terminal`	Enter configterminal mode
`(config)#vlan database`	Enter into the vlan database
`(config-vlan)# vlan 30 bridge 1 state enable`	Configure vlan 30 to bridge 1
`(config-vlan)#Exit`	Exit from the vlan database.
`(config)#int xe1`	Enter interface configuration mode for xe1
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`(config-if)#switchport mode trunk`	Set the switching characteristics of this interface as trunk
`(config-if)#switchport trunk allowed vlan add 30`	Configure vlan 30
`(config-if)#switchport protected isolated`	Configure interface as isolated port
`(config-if)#exit`	Exit from interface
`(config)#int xe2`	Enter interface configuration mode for xe2
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`(config-if)#switchport mode trunk`	Set the switching characteristics of this interface as trunk
`(config-if)#switchport trunk allowed vlan add 30`	Configure vlan 30
`(config-if)#switchport protected promiscuous`	Configure interface as promiscuous port
`(config-if)#exit`	Exit from interface mode
`(config)#commit`	Commit the configure on the node.

Validation

RTR1

```
#show running-config interface xe1
!
interface xe1
switchport
    switchport protected isolated
    bridge-group 1
    switchport mode trunk
    switchport trunk allowed vlan add 30
!
#show running-config interface xe2
!
interface xe2
 switchport
 switchport protected promiscuous
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan add 30
```

```
#show interface xe1
Interface xe1
  Flexport: Non Control Port (Active)
  Hardware is ETH  Current HW addr: 80a2.353f.edb7
  Physical:80a2.353f.edb7  Logical:(not set)
  Forward Error Correction (FEC) configured is Auto (default)
  FEC status is N/A
  Port Mode is trunk
  Protected Mode is Isolated
  Interface index: 5001
  Metric 1 mtu 1500 duplex-full link-speed 10g
  Debounce timer: disable
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
  Bandwidth 10g
  DHCP client is disabled.
  Last Flapped: 2022 Jan 06 13:13:42 (00:24:53 ago)
  Statistics last cleared: 2022 Jan 06 13:13:42 (00:24:53 ago)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 256 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 7 broadcast packets 0
    input packets 7 bytes 814
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 7
    Rx pause 0
  TX
    unicast packets 0 multicast packets 749 broadcast packets 0
    output packets 749 bytes 47944
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0

#show interface xe2
Interface xe2
  Flexport: Non Control Port (Active)
  Hardware is ETH  Current HW addr: 80a2.353f.edb9
  Physical:80a2.353f.edb9  Logical:(not set)
  Forward Error Correction (FEC) configured is Auto (default)
  FEC status is N/A
  Port Mode is trunk
  Protected Mode is Promiscuous
  Interface index: 5003
```

```
  Metric 1 mtu 1500 duplex-full link-speed 10g
  Debounce timer: disable
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
  Bandwidth 10g
  DHCP client is disabled.
  Last Flapped: Never
  Statistics last cleared: 2022 Jan 06 13:15:32 (00:23:52 ago)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 0 broadcast packets 0
    input packets 0 bytes 0
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 4569 broadcast packets 0
    input packets 4569 bytes 327802
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0
Send the vlan 30 tagged traffic from traffic 1 to traffic 2,
 #show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|  Interface|Rx mbps|Rx pps|Tx mbps|Tx pps|
+-------------------+--------------+-------------+--------------+-------------+
     Xe1     100.01     20   0.00     0
     Xe2      0.00      0    100.01   20


Send the vlan 30 tagged traffic from traffic 1 to traffic 2,
 #show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|  Interface|Rx mbps|Rx pps|Tx mbps|Tx pps|
+-------------------+--------------+-------------+--------------+-------------+
      Xe1     0.00     20    100.00  0
      Xe2     100.00   0     0.00    20
```

Isolated-Isolated Configuration

RTR1

Bridge Configuration:

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Configure bridge

VLAN Configuration:

`#configure terminal`	Enter configterminal mode
`(config)#vlan database`	Enter into the vlan database
`(config-vlan)# vlan 30 bridge 1 state enable`	Configure vlan 30 to bridge 1
`(config-vlan)#Exit`	Exit from the vlan database.
`(config)#int xe1`	Enter interface configuration mode for xe1
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`(config-if)#switchport mode trunk`	Set the switching characteristics of this interface as trunk
`(config-if)#switchport trunk allowed vlan add 30`	Configure vlan 30
`(config-if)#switchport protected isolated`	Configure interface as isolated port
`(config-if)#exit`	Exit from interface
`(config)#int xe2`	Enter interface configuration mode for xe2
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Associate interface with bridge-group 1
`(config-if)#switchport mode trunk`	Set the switching characteristics of this interface as trunk
`(config-if)#switchport trunk allowed vlan add 30`	Configure vlan 30
`(config-if)#switchport protected isolated`	Configure interface as isolated port
`(config-if)#exit`	Exit from interface mode
`(config)#commit`	Commit the configure on the node.

Validation

RTR1

```
#show running-config interface xe1
!
interface xe1
switchport
   switchport protected isolated
   bridge-group 1
```

```
    switchport mode trunk
    switchport trunk allowed vlan add 30
!
#show running-config interface xe2
!
interface xe2
 switchport
 switchport protected isolated
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan add 30

#show interface xe1
Interface xe1
  Flexport: Non Control Port (Active)
  Hardware is ETH  Current HW addr: 80a2.353f.edb7
  Physical:80a2.353f.edb7  Logical:(not set)
  Forward Error Correction (FEC) configured is Auto (default)
  FEC status is N/A
  Port Mode is trunk
  Protected Mode is Isolated
  Interface index: 5001
  Metric 1 mtu 1500 duplex-full link-speed 10g
  Debounce timer: disable
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
  Bandwidth 10g
  DHCP client is disabled.
  Last Flapped: 2022 Jan 06 13:13:42 (00:24:53 ago)
  Statistics last cleared: 2022 Jan 06 13:13:42 (00:24:53 ago)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 256 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 7 broadcast packets 0
    input packets 7 bytes 814
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 7
    Rx pause 0
  TX
    unicast packets 0 multicast packets 749 broadcast packets 0
    output packets 749 bytes 47944
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0
```

```
#show interface xe2
Interface xe2
  Flexport: Non Control Port (Active)
  Hardware is ETH  Current HW addr: 80a2.353f.edb9
  Physical:80a2.353f.edb9  Logical:(not set)
  Forward Error Correction (FEC) configured is Auto (default)
  FEC status is N/A
  Port Mode is trunk
  Protected Mode is Isolated
  Interface index: 5003
  Metric 1 mtu 1500 duplex-full link-speed 10g
  Debounce timer: disable
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
  Bandwidth 10g
  DHCP client is disabled.
  Last Flapped: Never
  Statistics last cleared: 2022 Jan 06 13:15:32 (00:23:52 ago)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 0 broadcast packets 0
    input packets 0 bytes 0
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 0 broadcast packets 0
    output packets 0 bytes 0
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0

Send the vlan 30 tagged traffic from traffic 1 to traffic 2,
#show interface counters rate mbps
+-------------------+--------------+-------------+--------------+-------------+
|  Interface|Rx mbps|Rx pps|Tx mbps|Tx pps|
+-------------------+--------------+-------------+--------------+-------------+
     Xe1      100.01   20    0.00     0
     Xe2      0.00     0     0.00     0
```

CHAPTER 27 MLAG with Provider Bridging Configuration

This chapter contains sample MLAG with Provider bridging configuration.

A provider bridged network is a virtual bridged Local Area Network that comprises provider bridges (SVLAN bridges and provider edge bridges) and attached LANs, under the administrative control of a single service provider. Provider bridges interconnect the separate MACs of the IEEE 802 LANs that compose a provider bridged network, relaying frames to provide connectivity between all the LANs that provide customer interfaces for each service instance.

MLAG (also called DRNI, Distributed Resilient Network Interconnect) expands the concept of link aggregation so that it provides node-level redundancy by allowing two or more nodes to share a common LAG endpoint. MLAG emulates multiple nodes to represent as a single logical node to the remote node running link aggregation. As a result, even if one of the nodes is down there exists a path to reach the destination through the other nodes.

Note: For MLAG with PB, use provider rstp edge bridge on TOR (PEB) nodes and LEAF (PB) node.

Configuration

Topology

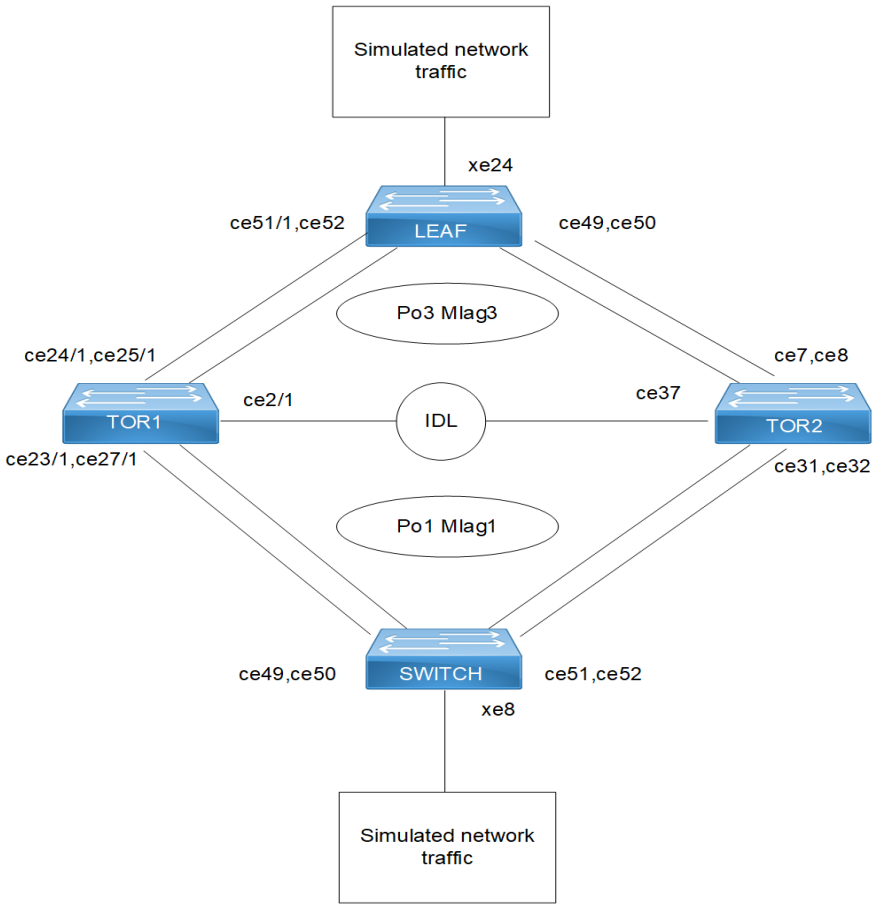


Figure 27-50: MLAG with Provider Bridging

Switch

SWITCH#configure terminal	Enter configuration mode
SWITCH(config)#bridge 1 protocol rstp vlan-bridge	Configure the rstp vlan bridge
SWITCH(config)#vlan database	Enter VLAN configuration mode
SWITCH(config-vlan)#vlan 2-2000 bridge 1 state enable	Create vlan for bridge
SWITCH(config-vlan)#exit	Exit VLAN configuration mode
SWITCH(config)#interface po1	Enter interface configuration mode for po1
SWITCH(config-if)#switchport	Configure switchport
SWITCH(config-if)#bridge-group 1 spanning-tree disable	Associate interface with bridge-group 1 by disblaing spanning tree
SWITCH(config-if)#switchport mode trunk	Configure switchport mode as trunk
SWITCH(config-if)#switchport trunk allowed vlan all	Associate created vlans to po1 interface
SWITCH(config-if)#exit	Exit from interface mode
SWITCH(config)#interface xe8	Enter interface configuration mode for xe8
SWITCH(config-if)#switchport	Configure switchport
SWITCH(config-if)#bridge-group 1 spanning-tree disable	Associate interface with bridge-group 1 by disblaing spanning tree
SWITCH(config-if)#switchport mode trunk	Configure switchport mode as trunk
SWITCH(config-if)#switchport trunk allowed vlan all	Associate created vlans to xe8 interface
SWITCH(config-if)#exit	Exit from interface mode
SWITCH(config)#interface ce49	Enter interface configuration mode for ce49
SWITCH(config-if)# channel-group 1 mode active	Configure interface as member port for po1- port channel
SWITCH(config-if)#exit	Exit from interface mode
SWITCH(config)#interface ce50	Enter interface configuration mode for ce49
SWITCH(config-if)#channel-group 1 mode active	Configure interface as member port for po1- port channel
SWITCH(config-if)#exit	Exit from interface mode
SWITCH(config)#interface ce51	Enter interface configuration mode for ce49
SWITCH(config-if)#channel-group 1 mode active	Configure interface as member port for po1- port channel
SWITCH(config-if)#exit	Exit from interface mode
SWITCH(config)#interface ce52	Enter interface configuration mode for ce49
SWITCH(config-if)#channel-group 1 mode active	Configure interface as member port for po1- port channel
SWITCH(config-if)#exit	Exit from interface mode
SWITCH(config)#commit	Commit the candidate configuration to the running configuration.
SWITCH(config)#exit	Exit from config mode

TOR1 (PEB)

`TOR1#configure terminal`	Enter configuration mode
`TOR1(config)#bridge 1 protocol provider-rstp edge`	Create provider rstp edge bridge
`TOR1(config)#vlan database`	Enter VLAN configuration mode
`TOR1(config-vlan)#vlan 2-500 type customer bridge 1 state enable`	Create customer vlan VLAN 2-500
`TOR1(config-vlan)#vlan 501-1005 type service point-point bridge 1 state enable`	Create service vlan VLAN 501-1005
`TOR1(config-vlan)#exit`	Exit VLAN configuration mode
`TOR1(config)#cvlan registration table cvlan100  bridge 1`	Create cvlan registration table with name cvlan100
`TOR1(config-cvlan-registration)#cvlan 100 svlan 1000`	Map cvlan100 with svlan 1000
`TOR1(config-cvlan-registration)#exit`	Exit registration table
`TOR1(config)#hardware-profile filter egress-l2 enable`	Enable the hardware-profile filter for egress l2.
`TOR1(config)#interface mlag1`	Enter interface configuration mode for mlag1
`TOR1(config-if)#switchport`	Configure switchport
`TOR1(config-if)#bridge-group 1 spanning-tree disable`	Associate interface with bridge-group 1 and disable spanning-tree
`TOR1(config-if)#switchport mode customer-edge trunk`	Configure switchport mode customer edge
`TOR1(config-if)# switchport customer-edge trunk allowed vlan add 100`	Associate customer vlan100 to interface
`TOR1(config-if)#switchport customer-edge vlan registration cvlan100`	Attach registration table cvlan100 to interface
`TOR1(config-if)#mode active-active`	Configure mlag mode as active-active
`TOR1(config-if)#exit`	Exit interface mode
`TOR1(config)#interface mlag3`	Enter interface configuration mode for mlag3
`TOR1(config-if)#switchport`	Make interface as switchport
`TOR1(config-if)# bridge-group 1 spanning-tree disable`	Associate interface with bridge-group 1 and disable spanning-tree
`TOR1(config-if)#switchport mode provider-network`	Configure switchport pnp port
`TOR1(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`TOR1(config-if)#mode active-active`	Configure mlag mode as active-active
`TOR1(config-if)#exit`	Exit interface configuration mode
`TOR1(config)#interface po1`	Enter interface configuration mode for po1
`TOR1(config-if)#switchport`	Make interface as switchport
`TOR1(config-if)#mlag 1`	Associate mlag1 interfacce to po1
`TOR1(config-if)#exit`	Exit interface configuration mode
`TOR1(config)#interface po3`	Enter interface configuration mode for po3
`TOR1(config-if)#switchport`	Make interface as switchport

TOR1(config-if)#dot1ad ethertype 0x88a8	Configure TPID with 88a8 to send and receive double tag (Q in Q)
TOR1(config-if)#mlag 3	Associate mlag3 interfacce to po3
TOR1(config-if)#exit	Exit interface configuration mode
TOR1(config)#interface ce2/1	Enter interface configuration mode for ce2/1 which is an IDL link
TOR1(config-if)#switchport	Make interface as switchport
TOR1(config-if)#exit	Exit interface configuration mode
TOR1(config)#interface ce24/1	Enter interface configuration mode for ce24/1
TOR1(config-if)#channel-group 3 mode active	Configure interface as member port for po3- port channel
TOR1(config-if)#exit	Exit interface configuration mode
TOR1(config)# interface ce25/1	Enter interface configuration mode for ce25/1
TOR1(config-if)#channel-group 3 mode active	Configure interface as member port for po3- port channel
TOR1(config-if)#exit	Exit interface configuration mode
TOR1(config)#interface ce23/1	Enter interface configuration mode for ce23/1
TOR1(config-if)#channel-group 1 mode active	Configure interface as member port for po1- port channel
TOR1(config-if)#exit	Exit interface configuration mode
TOR1(config)#interface ce27/1	Enter interface configuration mode for ce2471
TOR1(config-if)#channel-group 1 mode active	Configure interface as member port for po1- port channel
TOR1(config-if)#exit	Exit interface configuration mode
TOR1(config)#mcec domain configuration	Enter mcec domain configuration mode
TOR1(config-mcec-domain)#domain-address 2222.3333.4444	Configure domain address for mlag domain
TOR1(config-mcec-domain)#domain-system-number 1	Configure domain number to identify node in a domain
TOR1(config-mcec-domain)#intra-domain-link ce2/1	Configure intra domain link between tor nodes mlag domain
TOR1(config-mcec-domain)#exit	Exit from mcec domain mode
TOR1(config)#commit	Commit the candidate configuration to the running configuration.
TOR1(config)#exit	Exit from config mode

TOR2 (PEB)

TOR2#configure terminal	Enter configuration mode
TOR2(config)#bridge 1 protocol provider-rstp edge	Create provider rstp edge bridge
TOR2(config)#vlan database	Enter VLAN configuration mode
TOR2(config-vlan)#vlan 2-500 type customer bridge 1 state enable	Create customer vlan VLAN 2-500
TOR2(config-vlan)#vlan 501-1005 type service point-point bridge 1 state enable	Create service vlan VLAN 501-1005
TOR2(config-vlan)#exit	Exit VLAN configuration mode
TOR2(config)#cvlan registration table cvlan100 bridge 1	Create cvlan registration table with name cvlan100

TOR2(config-cvlan-registration)#cvlan 100 svlan 1000	Map cvlan100 with svlan 1000
TOR2(config-cvlan-registration)#exit	Exit registration table
TOR2(config)#hardware-profile filter egress-l2 enable	Enable the hardware-profile filter for egress l2.
TOR2(config)#interface mlag1	Enter interface configuration mode for mlag1
TOR2(config-if)#switchport	Configure switchport
TOR2(config-if)#bridge-group 1 spanning-tree disable	Associate interface with bridge-group 1 and disable spanning-tree
TOR2(config-if)#switchport mode customer-edge trunk	Configure switchport mode customer edge
TOR2(config-if)# switchport customer-edge trunk allowed vlan add 100	Associate customer vlan 100 to interface
TOR2(config-if)#switchport customer-edge vlan registration cvlan100	Attach registration table cvlan100 to interface
TOR2(config-if)#mode active-active	Configure mlag mode as active-active
TOR2(config-if)#exit	Exit interface mode
TOR2(config)#interface mlag3	Enter interface configuration mode for mlag3
TOR2(config-if)#switchport	Make interface as switchport
TOR2(config-if)# bridge-group 1 spanning-tree disable	Associate interface with bridge-group 1 and disable spanning-tree
TOR2(config-if)#switchport mode provider-network	Configure switchport pnp port
TOR2(config-if)#switchport provider-network allowed vlan all	Associate all svlan to the port
TOR2(config-if)#mode active-active	Configure mlag mode as active-active
TOR2(config-if)#exit	Exit interface configuration mode
TOR2(config)#interface po1	Enter interface configuration mode for po1
TOR2(config-if)#switchport	Make interface as switchport
TOR2(config-if)#mlag 1	Associate mlag1 interfacce to po1
TOR2(config-if)#exit	Exit interface configuration mode
TOR2(config)#interface po3	Enter interface configuration mode for po3
TOR2(config-if)#switchport	Make interface as switchport
TOR2(config-if)#dot1ad ethertype 0x88a8	Configure TPID with 88a8 to send and receive double tag (Q in Q)
TOR2(config-if)#mlag 3	Associate mlag1 interfacce to po3
TOR2(config-if)#exit	Exit interface configuration mode
TOR2(config)#interface ce37	Enter interface configuration mode for ce2/1 which is an IDL link
TOR2(config-if)#switchport	Make interface as switchport
TOR2(config-if)#exit	Exit interface configuration mode
TOR2(config)#interface ce7	Enter interface configuration mode for ce7
TOR2(config-if)#channel-group 3 mode active	Configure interface as member port for po3- port channel
TOR2(config-if)#exit	Exit interface configuration mode
TOR2(config)# interface ce8	Enter interface configuration mode for ce8

TOR2(config-if)#channel-group 3 mode active	Configure interface as member port for po3- port channel
TOR2(config-if)#exit	Exit interface configuration mode
TOR2(config)#interface ce31	Enter interface configuration mode for ce31
TOR2(config-if)#channel-group 1 mode active	Configure interface as member port for po1- port channel
TOR2(config-if)#exit	Exit interface configuration mode
TOR2(config)#interface ce32	Enter interface configuration mode for ce32
TOR2(config-if)#channel-group 1 mode active	Configure interface as member port for po1- port channel
TOR2(config-if)#exit	Exit interface configuration mode
TOR2(config)#mcec domain configuration	Enter mcec domain configuration mode
TOR2(config-mcec-domain)#domain-address 2222.3333.4444	Configure domain address for mlag domain
TOR2(config-mcec-domain)#domain-system-number 2	Configure domain number to identify node in a domain
TOR2(config-mcec-domain)#intra-domain-link ce37	Configure intra domain link between tor nodes mlag domain
TOR2(config-mcec-domain)#exit	Exit interface configuration mode
TOR2(config)#commit	Commit the candidate configuration to the running configuration.
TOR2(config)#exit	Exit interface configuration mode

LEAF(PB)

LEAF#configure terminal	Enter configuration mode
LEAF(config)# bridge 1 protocol provider-rstp edge	Create provider rstp edge bridge
LEAF(config)#vlan database	Enter VLAN configuration mode
LEAF(config-vlan)#vlan 2-500 type customer bridge 1 state enable	Create customer vlan VLAN 2-500
LEAF(config-vlan)#vlan 501-1005 type service point-point bridge 1 state enable	Create service vlan VLAN 501-1005
LEAF(config-vlan)#exit	Exit VLAN configuration mode
LEAF(config)#interface po3	Enter interface configuration mode for po3
LEAF(config-if)#switchport	Make interface as switchport
LEAF(config-if)#dot1ad ethertype 0x88a8	Configure TPID with 88a8 to send and receive double tag (Q in Q)
LEAF(config-if)#bridge-group 1 spanning-tree disable	Associate interface with bridge-group 1 and disable spanning-tree
LEAF(config-if)#switchport mode provider-network	Configure switchport pnp port
LEAF(config-if)#switchport provider-network allowed vlan all	Associate all svlan to the port
LEAF(config-if)#exit	Exit interface configuration mode
LEAF(config)#interface xe24	Enter interface configuration mode for xe24
LEAF(config-if)#switchport	Make interface as switchport
LEAF(config-if)#dot1ad ethertype 0x88a8	Configure TPID with 88a8 to send and receive double tag (Q in Q)

`LEAF(config-if)#bridge-group 1 spanning-tree disable`	Associate interface with bridge-group 1 and disable spanning-tree
`LEAF(config-if)#switchport mode provider-network`	Configure switchport pnp port
`LEAF(config-if)#switchport provider-network allowed vlan all`	Associate all svlan to the port
`LEAF(config-if)#exit`	Exit interface configuration mode
`LEAF(config)#interface ce49`	Enter interface configuration mode for ce49
`LEAF(config-if)# channel-group 3 mode active`	Configure interface as member port for po3- port channel
`LEAF(config-if)#exit`	Exit interface configuration mode
`LEAF(config)#interface ce50`	Enter interface configuration mode for ce50
`LEAF(config-if)# channel-group 3 mode active`	Configure interface as member port for po3- port channel
`LEAF(config-if)#exit`	Exit interface configuration mode
`LEAF(config)#interface ce51`	Enter interface configuration mode for ce51
`LEAF(config-if)# channel-group 3 mode active`	Configure interface as member port for po3- port channel
`LEAF(config-if)#exit`	Exit interface configuration mode
`LEAF(config)#interface ce52`	Enter interface configuration mode for ce52
`LEAF(config-if)# channel-group 3 mode active`	Configure interface as member port for po3- port channel
`LEAF(config-if)#exit`	Exit interface configuration mode
`LEAF(config)#commit`	Commit the candidate configuration to the running configuration.
`LEAF(config)#exit`	Exit from config mode

Validation

Validation commands are : `show mlag domain summary , show mlag domain details, show ether-channel summary, show bridge, Show mac address-table bridge <bridge-id>, show cvlan registration table bridge <bridge-id>`

For below show mac table output sending cvlan 100 traffic from SWITCH to LEAF, for which TOR nodes add svlan 1000 and egress same to LEAF and LEAF ixia also receives double tag.

```
TOR1#show mlag domain details

------------------------------------
Domain Configuration
------------------------------------

Domain System Number           : 1
Domain Address                 : 2222.3333.4444
Domain Priority                : 32768
Intra Domain Interface         : ce2/1

Hello RCV State                : Current
Hello Periodic Timer State     : Slow Periodic
Domain Sync                    : IN_SYNC
```

```
Neigh Domain Sync              : IN_SYNC
Domain Adjacency               : UP
Domain Sync via                : Intra-domain-interface

-----------------------------------
MLAG Configuration
-----------------------------------

MLAG-1
  Mapped Aggregator            : po1
  Admin Key                    : 16385
  Oper Key                     : 16385
  Physical status              : 1
  Physical properties Digest   : 1b bc c2 24 5a 1c cf 6 88 32 a1 4b 62 c2 c0 2

  Neigh Admin Key              : 32769
  Neigh Physical status        : 1
  Neigh Physical Digest        : 1b bc c2 24 5a 1c cf 6 88 32 a1 4b 62 c2 c0 2
  Info RCV State               : Current
  Info Periodic Time State     : Standby
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Active
  Current Mlag state           : Active

MLAG-3
  Mapped Aggregator            : po3
  Admin Key                    : 16387
  Oper Key                     : 16387
  Physical status              : 1
  Physical properties Digest   : 46 51 95 9d e2 90 81 47 d0 51 d9 de 4f 8 48 93

  Neigh Admin Key              : 32771
  Neigh Physical status        : 1
  Neigh Physical Digest        : 46 51 95 9d e2 90 81 47 d0 51 d9 de 4f 8 48 93
  Info RCV State               : Current
  Info Periodic Time State     : Standby
  Mlag Sync                    : IN_SYNC
  Mode                         : Active-Active
  Current Mlag state           : Active

TOR1#

TOR1#show mlag domain summary

-----------------------------------
Domain Configuration
-----------------------------------

Domain System Number            : 1
Domain Address                  : 2222.3333.4444
```

```
Domain Priority                 : 32768
Intra Domain Interface          : ce2/1
Domain Adjacency                : UP
Domain Sync via                 : Intra-domain-interface
-----------------------------------
MLAG Configuration
-----------------------------------

MLAG-1
  Mapped Aggregator             : po1
  Physical properties Digest    : 1b bc c2 24 5a 1c cf 6 88 32 a1 4b 62 c2 c0 2
  Total Bandwidth               : 400g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active-Active
  Current Mlag state            : Active


MLAG-3
  Mapped Aggregator             : po3
  Physical properties Digest    : 46 51 95 9d e2 90 81 47 d0 51 d9 de 4f 8 48 93
  Total Bandwidth               : 400g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active-Active
  Current Mlag state            : Active


TOR1#

TOR1#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 16385 - Oper Key 16385
     Link: ce23/1 (5001) sync: 1 (Mlag-active-link)
     Link: ce27/1 (5029) sync: 1 (Mlag-active-link)
-------------------------------------
  Aggregator po3 100003
  Aggregator Type: Layer2
  Admin Key: 16387 - Oper Key 16387
     Link: ce25/1 (5005) sync: 1 (Mlag-active-link)
     Link: ce24/1 (5117) sync: 1 (Mlag-active-link)
TOR1#

TOR2#show mlag domain details

-----------------------------------
Domain Configuration
-----------------------------------

Domain System Number            : 2
Domain Address                  : 2222.3333.4444
```

```
Domain Priority               : 32768
Intra Domain Interface        : ce37

Hello RCV State               : Current
Hello Periodic Timer State    : Slow Periodic
Domain Sync                   : IN_SYNC
Neigh Domain Sync             : IN_SYNC
Domain Adjacency              : UP
Domain Sync via               : Intra-domain-interface

-----------------------------------
MLAG Configuration
-----------------------------------

MLAG-1
  Mapped Aggregator           : po1
  Admin Key                   : 32769
  Oper Key                    : 16385
  Physical status             : 1
  Physical properties Digest  : 1b bc c2 24 5a 1c cf 6 88 32 a1 4b 62 c2 c0 2

  Neigh Admin Key             : 16385
  Neigh Physical status       : 1
  Neigh Physical Digest       : 1b bc c2 24 5a 1c cf 6 88 32 a1 4b 62 c2 c0 2
  Info RCV State              : Current
  Info Periodic Time State    : Standby
  Mlag Sync                   : IN_SYNC
  Mode                        : Active-Active
  Current Mlag state          : Active

MLAG-3
  Mapped Aggregator           : po3
  Admin Key                   : 32771
  Oper Key                    : 16387
  Physical status             : 1
  Physical properties Digest  : 46 51 95 9d e2 90 81 47 d0 51 d9 de 4f 8 48 93

  Neigh Admin Key             : 16387
  Neigh Physical status       : 1
  Neigh Physical Digest       : 46 51 95 9d e2 90 81 47 d0 51 d9 de 4f 8 48 93
  Info RCV State              : Current
  Info Periodic Time State    : Standby
  Mlag Sync                   : IN_SYNC
  Mode                        : Active-Active
  Current Mlag state          : Active

TOR2#  show mlag domain summary

-----------------------------------
Domain Configuration
```

```
-------------------------------------

Domain System Number            : 2
Domain Address                  : 2222.3333.4444
Domain Priority                 : 32768
Intra Domain Interface          : ce37
Domain Adjacency                : UP
Domain Sync via                 : Intra-domain-interface
-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
  Mapped Aggregator             : po1
  Physical properties Digest    : 1b bc c2 24 5a 1c cf 6 88 32 a1 4b 62 c2 c0 2
  Total Bandwidth               : 400g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active-Active
  Current Mlag state            : Active


MLAG-3
  Mapped Aggregator             : po3
  Physical properties Digest    : 46 51 95 9d e2 90 81 47 d0 51 d9 de 4f 8 48 93
  Total Bandwidth               : 400g
  Mlag Sync                     : IN_SYNC
  Mode                          : Active-Active
  Current Mlag state            : Active
TOR2#

TOR2#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 32769 - Oper Key 16385
     Link: ce31 (5062) sync: 1 (Mlag-active-link)
     Link: ce32 (5064) sync: 1 (Mlag-active-link)
-------------------------------------
  Aggregator po3 100003
  Aggregator Type: Layer2
  Admin Key: 32771 - Oper Key 16387
     Link: ce7 (5029) sync: 1 (Mlag-active-link)
     Link: ce8 (5031) sync: 1 (Mlag-active-link)
TOR2#

SWITCH2#show bridge
bridge 1 is running on rstp vlan-bridge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
```

```
  1         100                  xe8         0000.2223.2425    1     300
SWITCH2#
SWITCH2#
SWITCH2#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
  100          0000.2223.2425  dynamic   xe8       Disable
SWITCH2#


TOR1# show bridge
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
1                1000          mlag1       0000.2223.2425    1     300
TOR1#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
       1000   0000.2223.2425  dynamic   mlag1     Disable
TOR1#


TOR2#show bridge
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
  1                1000          mlag1       0000.2223.2425    1     300
TOR2#

TOR2#
TOR2#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
       1000   0000.2223.2425  dynamic   mlag1     Disable
TOR2#




LEAF#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
       1000   0000.2223.2425  dynamic   po3       Disable
```

```
LEAF#



LEAF#show bridge
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1                1000          po3         0000.2223.2425    1     300
LEAF#


Now send traffic with svlan-1000 and c-vlan 100 from LEAF to SWITCH,Tor removes svlan
and send only cvlan to SWITCH

LEAF#show bridge
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1                1000          po3         0000.2223.2425    1     300
 1                1000          xe24        0000.2425.2627    1     300
LEAF#

LEAF#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
       1000   0000.2223.2425  dynamic   po3       Disable
       1000   0000.2425.2627  dynamic   xe24      Disable
LEAF#


TOR1#show bridge
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 1                1000          mlag1       0000.2223.2425    1     300
 1                1000          mlag3       0000.2425.2627    1     300
TOR1#

TOR1#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+---------------+---------+---------+--------------
       1000   0000.2223.2425  dynamic   mlag1     Disable
       1000   0000.2425.2627  dynamic   mlag3     Disable
TOR1#
```

```
TOR2#show bridge
bridge 1 is running on provider-rstp edge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 --------+------+------+------+-----------+-----------------+-----+---------+
 1                1000          mlag1       0000.2223.2425    1     300
 1                1000          mlag3       0000.2425.2627    1     300
TOR2#

TOR2#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+--------------+---------+---------+--------------
       1000   0000.2223.2425  dynamic   mlag1     Disable
       1000   0000.2425.2627  dynamic   mlag3     Disable
TOR2#


SWITCH2#show bridge
bridge 1 is running on rstp vlan-bridge
Ageout time is global and if something is configured for vxlan then it will be a
ffected here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 --------+------+------+------+-----------+-----------------+-----+---------+
 1         100                 xe8         0000.2223.2425    1     300
 1         100                 po1         0000.2425.2627    1     300
SWITCH2#

SWITCH2#show mac address-table bridge 1
CVLAN  SVLAN  MAC Address     Type      Ports     Port-security
------+------+--------------+---------+---------+--------------
 100          0000.2223.2425  dynamic   xe8       Disable
 100          0000.2425.2627  dynamic   po1       Disable
SWITCH2#
```

L2CP with MLAG-Provider Bridging Configuring

Switch

SWITCH#configure terminal	Enter configuration mode
SWITCH(config)#interface xe8	Enter interface configuration mode for xe8
SWITCH(config-if)#switchport	Configure switchport
SWITCH(config-if)#bridge-group 1 spanning-tree disable	Associate interface with bridge-group 1 by disblaing spanning tree
SWITCH(config-if)#switchport mode trunk	Configure switchport mode as trunk
SWITCH(config-if)#switchport trunk allowed vlan all	Associate created vlans to xe8 interface
SWITCH(config-if)#l2protocol stp/lldp/elmi/efm/dot1x tunnel	Configure STP/LLDP/ELMI/EFM/dot1x protocol as Tunnel
SWITCH(config-if)#l2protocol stp tunnel	Configure STP protocol as Tunnel
SWITCH(config-if)#l2protocol lldp tunnel	Configure LLDP protocol as Tunnel
SWITCH(config-if)#l2protocol elmi tunnel	Configure ELMI protocol as Tunnel
SWITCH(config-if)#l2protocol efm tunnel	Configure EFM protocol as Tunnel
SWITCH(config-if)#l2protocol dot1x tunnel	Configure dot1x protocol as Tunnel
SWITCH(config-if)#exit	Exit from interface mode
SWITCH(config)#commit	Commit the candidate configuration to the running configuration.

TOR1 (PEB)

TOR1#configure terminal	Enter configuration mode
TOR1(config)#interface mlag1	Enter interface configuration mode for mlag1
TOR1(config-if)#switchport	Configure switchport
TOR1(config-if)#bridge-group 1 spanning-tree disable	Associate interface with bridge-group 1 and disable spanning-tree
TOR1(config-if)#switchport mode customer-edge trunk	Configure switchport mode customer edge
TOR1(config-if)# switchport customer-edge trunk allowed vlan add 100	Associate customer vlan100 to interface
TOR1(config-if)#switchport customer-edge vlan registration cvlan100	Attach registration table cvlan100 to interface
TOR1(config-if)#mode active-active	Configure mlag mode as active-active
TOR1(config-if)#l2protocol stp/lldp/elmi/efm/dot1x tunnel/peer/discard	Configure STP/LLDP/ELMI/EFM/dot1x protocol as tunnel/peer/discard

SWITCH(config-if)#l2protocol stp tunnel	Configure STP protocol as Tunnel
SWITCH(config-if)#l2protocol lldp tunnel	Configure LLDP protocol as Tunnel
SWITCH(config-if)#l2protocol elmi tunnel	Configure ELMI protocol as Tunnel
SWITCH(config-if)#l2protocol efm tunnel	Configure EFM protocol as Tunnel
SWITCH(config-if)#l2protocol dot1x tunnel	Configure dot1x protocol as Tunnel
TOR1(config-if)#exit	Exit interface mode
TOR1(config)#commit	Commit the candidate configuration to the running configuration.

TOR2 (PEB)

TOR2#configure terminal	Enter configuration mode
TOR2(config)#interface mlag1	Enter interface configuration mode for mlag1
TOR2(config-if)#switchport	Configure switchport
TOR2(config-if)#bridge-group 1 spanning-tree disable	Associate interface with bridge-group 1 and disable spanning-tree
TOR2(config-if)#switchport mode customer-edge trunk	Configure switchport mode customer edge
TOR2(config-if)# switchport customer-edge trunk allowed vlan add 100	Associate customer vlan100 to interface
TOR2(config-if)#switchport customer-edge vlan registration cvlan100	Attach registration table cvlan100 to interface
TOR2(config-if)#mode active-active	Configure mlag mode as active-active
TOR2(config-if)#l2protocol stp/lldp/elmi/ efm/dot2x tunnel/peer/discard	Configure STP/LLDP/ELMI/EFM/dot1x protocol as tunnel/ peer/discard
SWITCH(config-if)#l2protocol stp tunnel	Configure STP protocol as Tunnel
SWITCH(config-if)#l2protocol lldp tunnel	Configure LLDP protocol as Tunnel
SWITCH(config-if)#l2protocol elmi tunnel	Configure ELMI protocol as Tunnel
SWITCH(config-if)#l2protocol efm tunnel	Configure EFM protocol as Tunnel
SWITCH(config-if)#l2protocol dot1x tunnel	Configure dot1x protocol as Tunnel
TOR2(config-if)#exit	Exit interface mode
TOR2(config)#commit	Commit the candidate configuration to the running configuration.

Validation

Switch:

```
SWITCH#show l2protocol processing interface xe8
Bridge   Interface Name  Protocol     Processing Status     Hardware Status
```

```
======   ==============  ========     =================     ===============
1        xe8             stp          Tunnel                Tunnel
1        xe8             lacp         None                  Peer
1        xe8             dot1x        Tunnel                Tunnel
1        xe8             lldp         Tunnel                Tunnel
1        xe8             efm          Tunnel                Tunnel
1        xe8             elmi         Tunnel                Tunnel
```

TOR1:

```
TOR1#show l2protocol processing interface mlag1
Bridge   Interface Name  Protocol     Processing Status     Hardware Status
======   ==============  ========     =================     ===============
1        mlag1           stp          Tunnel                -
1        mlag1           lacp         None                  -
1        mlag1           dot1x        Discard               -
1        mlag1           lldp         Tunnel                -
1        mlag1           efm          Discard               -
1        mlag1           elmi         Peer                  -
1        mlag1           synce        None                  -



TOR1#show l2protocol processing interface ce23/1
Bridge   Interface Name  Protocol     Processing Status     Hardware Status
======   ==============  ========     =================     ===============
1        ce23/1          stp          Tunnel                Tunnel
1        ce23/1          lacp         None                  Peer
1        ce23/1          dot1x        Discard               Discard
1        ce23/1          lldp         Tunnel                Tunnel
1        ce23/1          efm          Discard               Discard
1        ce23/1          elmi         Peer                  Peer
1        ce23/1          synce        None                  Peer


TOR1#show l2protocol interface mlag1 counters
Interface mlag1
Tunnel                 :  stp                 : 241782
```

TOR2:

```
TOR2#show l2protocol processing interface mlag1
Bridge   Interface Name  Protocol     Processing Status     Hardware Status
======   ==============  ========     =================     ===============
1        mlag1           stp          Tunnel                -
1        mlag1           lacp         None                  -
1        mlag1           dot1x        Discard               -
1        mlag1           lldp         Tunnel                -
```

```
1        mlag1           efm          Discard              -
1        mlag1           elmi         Peer                 -
1        mlag1           synce        None                 -


TOR2#show l2protocol processing interface ce32
Bridge   Interface Name  Protocol     Processing Status    Hardware Status
======   ==============  ========     =================    ===============
1        ce32            stp          Tunnel               Tunnel
1        ce32            lacp         None                 Peer
1        ce32            dot1x        Discard              Discard
1        ce32            lldp         Tunnel               Tunnel
1        ce32            efm          Discard              Discard
1        ce32            elmi         Peer                 Peer
1        ce32            synce        None                 Peer
```

CHAPTER 28 Support IGMP Snooping for Provider Bridge

Overview

In Layer-2 switches, multicast IP traffic is handled in the same manner as broadcast traffic and forwards frames received on one interface to all other interfaces. This creates excessive traffic on the network, and affects network performance. The Internet Group Management Protocol (IGMP) Snooping allows switches to monitor network traffic, and determine hosts to receive multicast traffic. Thus, at a time only an host's membership report is relayed from a group instead of a report from each host in the group.

A Provider Bridge (PB) network is a virtual bridge Local Area Network (LAN) that comprises of Service provider bridges (SVLAN and PB) and attached LANs controlled under a single service provider administration. Provider bridges interconnect the MACs of the IEEE 802 LANs separately. This combined provider bridged network relay frames to all the connected LANs that provide customer interfaces for each service instance.

Feature Characteristics

The existing IGMP Snooping extended to support in the Provider Bridged (PB) network. The PB connects customer LANs using the switched provider network consisting of SVLAN bridges and provider edge bridges. Each customer LAN is connected to a separate service VLAN inside the provider network. Current release supports the IGMPv1/ IGMPv2/IGMPv3.

The following are supported:

- Snooping entries are captured in provider bridge network
- Egress traffic from router is tagged with single SVLAN ID
- IGMP snooping feature supported only in SVLAN

Benefits

This feature enables a Provider bridging network service provider to conserve bandwidth by efficiently switching the multicast packets.

Prerequisites

IGMP snooping is available over a number of network underlays. In this chapter, it is assumed that Provider Bridge support is configured.

Configuration

Topology

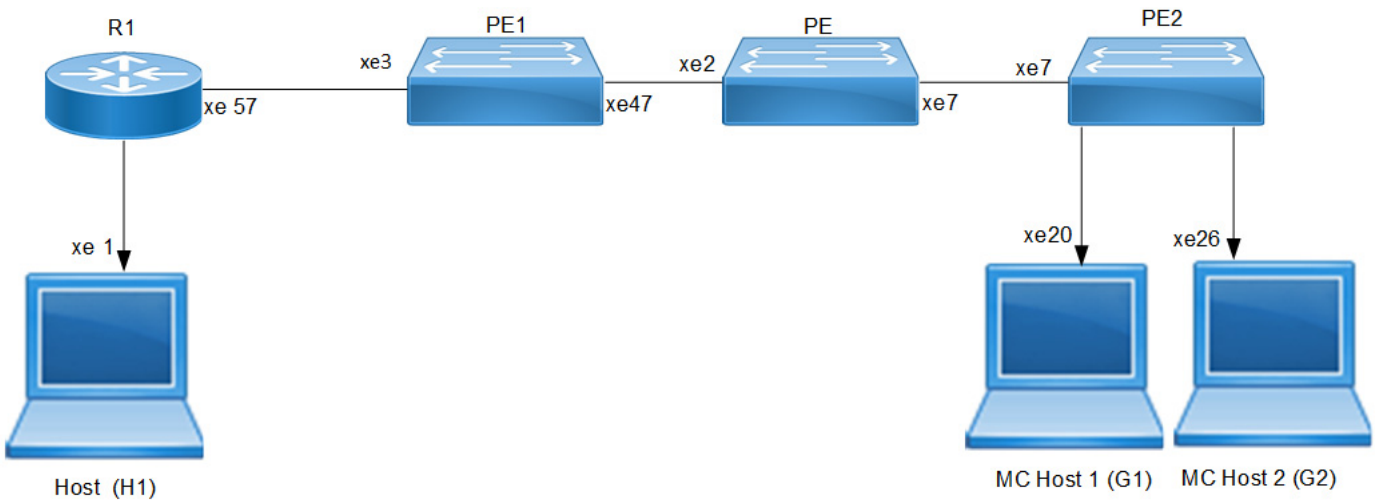


Figure 28-51: IGMP Snooping Provider Bridge Topology

R1

`#configure terminal`	Enter the configure mode.
`R1(config)#bridge 1 protocol provider-rstp edge`	Configure bridge `1` to the spanning-tree table.
`R1(config)#vlan database`	Configure the VLAN database.
`R1(config)#vlan 2 type service point-point bridge 1 state enable`	Configure the SVLAN 2 to bridge 1.
`R1(config)#ip multicast-routing`	Configure the multicast routing on the router.
`R1(config)#ip pim rp-address 1.1.1.1`	Configure Rendezvous Point (RP) address for multicast groups.
`R1(config)#interface lo`	Enter into lo interface.
`R1(config-if)#ip address 1.1.1.1/24 secondary`	Configure rp address as secondary.
`R1(config-if)#ip pim sparse-mode`	Enable the PIM sparse mode.
`R1(config-if)#exit`	Exit the loopback interface mode.
`R1(config)#interface svlan1.2`	Create the SVLAN interface.
`R1(config-if)#ip address 20.1.1.1/24`	Configure IPv4 address to VLAN interface.
`R1(config-if)#ip pim sparse-mode`	Configure PIM sparse mode.
`R1(config-if)#exit`	Exit the SVLAN interface mode.
`R1(config)#interface xe1`	Enter interface mode.
`R1(config-if)#ip address 10.1.1.1/24`	Configure IPv4 address to interface
`R1(config-if)#ip pim sparse-mode`	Configure PIM sparse mode.
`R1(config-if)#commit`	Commit the configurations.
`R1(config-if)#exit`	Exit the interface mode.
`R1(config)#interface xe57`	Enter interface mode.
`R1(config-if)#switchport`	Configure switchport.
`R1(config-if)#dot1ad ethertype 0x8100`	Configure ether type 0x8100.
`R1(config-if)#bridge-group 1 spanning-tree disable`	Configure bridge group.
`R1(config-if)#switchport mode provider-network`	Configure switchport trunk mode.
`R1(config-if)#switchport provider-network allowed vlan add 2`	Configure the VLAN to switchport trunk mode.
`R1(config-if)#commit`	Commit configurations

PE1

`#configure terminal`	Enter the configure mode.
`PE1(config)#bridge 1 protocol provider-rstp edge`	Configure bridge `1` to the spanning-tree table.

`PE1(config)#vlan database`	Configure the VLAN database.
`PE1(config)#vlan 2 type service point-point bridge 1 state enable`	Configure the SVLAN 2 to bridge 1.
`PE1(config)#ip multicast-routing`	Configure the multicast routing on the router.
`PE1(config)#interface svlan1.2`	Create VLAN interface.
`PE1(config-if)#igmp snooping enable`	Configure IPv4 address to VLAN interface .
`PE1PE1(config-if)#exit`	Exit the interface mode.
`PE1(config)#interface xe3`	Enter interface mode.
`PE1(config-if)#switchport`	Configure Switchport.
`PE1(config-if)#dot1ad ethertype 0x8100`	Configure ethertype.
`PE1(config-if)#bridge-group 1 spanning-tree disable`	Configure bridge group spanning tree disable .
`PE1(config-if)#switchport mode provider-network`	Configure provider network .
`PE1(config-if)#switchport provider-network allowed vlan add 2`	Configure the SVLAN to interface .
`PE1(config-if)#commit`	Commit configurations.
`PE1(config-if)#exit`	Exit the interface mode.
`PE1(config)#interface xe47`	Enter interface mode.
`PE1(config-if)#switchport`	Configure switchport
`PE1(config-if)#dot1ad ethertype 0x8100`	Configure ethertype.
`PE1(config-if)#bridge-group 1 spanning-tree disable`	Configure bridge group spanning tree disable.
`PE1(config-if)#switchport mode provider-network`	Configure provider network.
`PE1(config-if)#switchport provider-network allowed vlan add 2`	Configure service vlan to provider network.
`PE1(config-if)#commit`	Commit configurations.
`PE1(config-if)#exit`	Exit the interface mode.

PE

`#configure terminal`	Enter the configure mode.
`PE(config)#bridge 1 protocol provider-rstp edge`	Configure bridge `1` to the spanning-tree table.
`PE(config)#vlan database`	Configure the VLAN database
`PE(config)#vlan 2 type service point-point bridge 1 state enable`	Configure the SVLAN 2 to bridge 1.
`PE(config)#ip multicast-routing`	Configure the multicast routing on the router.
`PE(config)#interface svlan1.2`	Create VLAN interface.
`PE(config-if)#igmp snooping enable`	Configure IPv4 address to VLAN interface.
`PE(config-if)#exit`	Exit the interface mode.
`PE(config)#interface xe2`	Enter interface mode.
`PE(config-if)#switchport`	Configure Switchport
`PE(config-if)#dot1ad ethertype 0x8100`	Configure ethertype
`PE(config-if)#bridge-group 1 spanning-tree disable`	Configure bridge group spanning tree disable.
`PE(config-if)#switchport mode provider-network`	Configure provider network.
`PE(config-if)#switchport provider-network allowed vlan add 2`	Configure the SVLAN to interface.
`PE(config-if)#commit`	Commit configurations.
`PE(config-if)#exit`	Exit the interface mode.
`PE(config)#interface xe7`	Enter interface mode.
`PE(config-if)#switchport`	Configure switchport.
`PE(config-if)#dot1ad ethertype 0x8100`	Configure ethertype.
`PE(config-if)#bridge-group 1 spanning-tree disable`	Configure bridge group spanning tree disable.
`PE(config-if)#switchport mode provider-network`	Configure provider network.
`PE(config-if)#switchport provider-network allowed vlan add 2`	Configure service vlan to provider network.
`PE(config-if)#commit`	Commit configurations.
`PE(config-if)#exit`	Exit the interface mode.

PE2

`#configure terminal`	Enter the configure mode.
`PE2(config)#bridge 1 protocol provider-rstp edge`	Configure bridge `1` to the spanning-tree table.
`PE2(config)#vlan database`	Configure the VLAN database.
`PE2(config)#vlan 2 type service point-point bridge 1 state enable`	Configure the SVLAN 2 to bridge 1.
`PE2(config)#ip multicast-routing`	Configure the multicast routing on the router.
`PE2(config)#interface svlan1.2`	Create VLAN interface.
`PE2(config-if)#igmp snooping enable`	Enable the IGMP snooping on VLAN interface.
`PE2(config-if)#exit`	Exit the VLAN interface mode.
`PE2(config)#interface xe7`	Enter interface mode.
`PE2(config-if)#switchport`	Configure Switchport.
`PE2(config-if)#dot1ad ethertype 0x8100`	Configure ethertype.
`PE2(config-if)#bridge-group 1 spanning-tree disable`	Configure bridge group spanning tree disable.
`PE2(config-if)#switchport mode provider-network`	Configure provider network.
`PE2(config-if)#switchport provider-network allowed vlan add 2`	Configure the SVLAN to interface.
`PE2(config-if)#commit`	Commit configurations.
`PE2(config-if)#exit`	Exit the interface mode.
`PE2(config)#interface xe20`	Enter interface mode.
`PE2(config-if)#switchport`	Configure switchport.
`PE2(config-if)#dot1ad ethertype 0x8100`	Configure ethertype.
`PE2(config-if)#bridge-group 1 spanning-tree disable`	Configure bridge group spanning tree disable.
`PE2(config-if)#switchport mode provider-network`	Configure provider network.
`PE2(config-if)#switchport provider-network allowed vlan add 2`	Configure service VLAN to provider network.
`PE2(config-if)#commit`	Commit configurations.
`PE2(config-if)#exit`	Exit the interface mode.
`PE2(config)#interface xe22`	Enter interface mode.
`PE2(config-if)#switchport`	Configure switchport.
`PE2(config-if)#dot1ad ethertype 0x8100`	Configure ethertype.
`PE2(config-if)#bridge-group 1 spanning-tree disable`	Configure bridge group spanning tree disable.

`PE2(config-if)#switchport mode provider-network`	Configure provider network.
`PE2(config-if)#switchport provider-network allowed vlan add 2`	Configure service VLAN to provider network.
`PE2(config-if)#commit`	Commit configurations.
`PE2(config-if)#exit`	Exit the interface mode.

Validation

R1

```
MCRTR#show ip igmp groups
IGMP Instance wide G-Recs Count is: 2
IGMP Connected Group Membership
Group Address    Interface            Uptime     Expires   State    Last Reporter
231.1.1.1        svlan1.2             00:00:12   00:04:07  Active   0.0.0.0
231.1.1.2        svlan1.2             00:00:12   00:04:07  Active   0.0.0.0
MCRTR#
MCRTR#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
G/prefix Entries: 0
(*,G) Entries: 2
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0

(*, 231.1.1.1)
RP: 1.1.1.1
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 Local     ..i.............................
 Joined    ................................
 Asserted  ................................
FCR:

(*, 231.1.1.2)
RP: 1.1.1.1
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 Local     ..i.............................
 Joined    ................................
 Asserted  ................................
FCR:

MCRTR#
```

PE1

```
PEB1-7014#show igmp snooping interface
Global IGMP Snooping information
 IGMP Snooping Enabled
 IGMPv1/v2 Report suppression Enabled
 IGMPv3 Report suppression Enabled

IGMP Snooping information for svlan1.2
 IGMP Snooping enabled
 Snooping Querier none
 IGMP Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 IGMPv2 fast-leave is disabled
 IGMPv1/v2 Report suppression enabled
 IGMPv3 Report suppression enabled
 Router port detection using IGMP Queries
 Number of router-ports: 1
 Number of Groups: 0
 Number of v1-reports: 0
 Number of v2-reports: 0
 Number of v2-leaves: 0
 Number of v3-reports: 0
 Active Ports:
  xe3
  xe47
PEB1-7014#show igmp snooping groups
IGMP Instance wide G-Recs Count is: 2
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static, > - Hw Installed)
Vlan   Group/Source Address    Interface      Flags   Uptime      Expires  Last Reporter     Version
2      231.1.1.1              xe47           R    >  00:07:15    00:03:48 0.0.0.0           V3
2      231.1.1.2              xe47           R    >  00:07:15    00:03:48 0.0.0.0           V3
PEB1-7014#
```

PE

```
PB-7024#show igmp snooping interface
Global IGMP Snooping information
 IGMP Snooping Enabled
 IGMPv1/v2 Report suppression Enabled
 IGMPv3 Report suppression Enabled

IGMP Snooping information for svlan1.2
 IGMP Snooping enabled
 Snooping Querier none
 IGMP Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 IGMPv2 fast-leave is disabled
 IGMPv1/v2 Report suppression enabled
 IGMPv3 Report suppression enabled
```

```
 Router port detection using IGMP Queries
 Number of router-ports: 1
 Number of Groups: 0
 Number of v1-reports: 0
 Number of v2-reports: 0
 Number of v2-leaves: 0
 Number of v3-reports: 0
 Active Ports:
  xe7
  xe2
PB-7024#
PB-7024#show igmp snooping groups
IGMP Instance wide G-Recs Count is: 2
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static, > - Hw Installed)
Vlan   Group/Source Address    Interface     Flags   Uptime
Expires  Last Reporter     Version
2      231.1.1.1              xe7           R    >  00:07:15        00:03:45 20.1.1.2          V3
2      231.1.1.2              xe7           R    >  00:07:15        00:03:51 20.1.1.3          V3
PB-7024#
```

PE2

```
PEB2-7019#show igmp snooping interface
Global IGMP Snooping information
 IGMP Snooping Enabled
 IGMPv1/v2 Report suppression Disabled
 IGMPv3 Report suppression Disabled

IGMP Snooping information for svlan1.2
 IGMP Snooping enabled
 Snooping Querier none
 IGMP Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 IGMPv2 fast-leave is disabled
 IGMPv1/v2 Report suppression disabled
 IGMPv3 Report suppression disabled
 Router port detection using IGMP Queries
 Number of router-ports: 1
 Number of Groups: 0
 Number of v1-reports: 0
 Number of v2-reports: 0
 Number of v2-leaves: 0
 Number of v3-reports: 0
 Active Ports:
  xe20
  xe26
  xe7
    PEB2-7019#
    PEB2-7019#show igmp snooping groups
    IGMP Instance wide G-Recs Count is: 2
    IGMP Snooping Group Membership
```

```
     Group source list: (R - Remote, S - Static, > - Hw Installed)
Vlan  Group/Source Address   Interface    Flags  Uptime Expires Last Reporter   Version
2      231.1.1.1              xe20          R    >  00:07:14  00:03:45 20.1.1.2          V3
2      231.1.1.2              xe26          R    >  00:07:15  00:03:51 20.1.1.3       V3
PEB2-7019#
```

Abbreviations

Table 28-6:

Acronym	Description
IGMP	Internet Group Management Protocol
PB	Provider Bridged
SVLAN	Service Provider VLAN

Layer 2 Command Reference

CHAPTER 1 Link Layer Discovery Protocol v2 Commands

The commands in this chapter support:

- Link Layer Discovery Protocol (LLDP) version 2 as described in IEEE 802.1AB 2009
- LLDP-MED protocol extension as per ANSI/TIA-1057 April 2006.

Note: To enable LLDPv2, LLDP (previous version) should be disabled or vice versa.

clear lldp counters

Use this command to clear the LLDP statistics on all the interfaces.

Command Syntax

```
clear lldp counters
```

Parameters

`counters`	Reset the LLDP traffic counters to zero.

Command Mode

Exec Mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear lldp counters
```

clear lldp neighbors

Use this command to clear the learned lldp neighbors information.

Command Syntax

```
clear lldp neighbors (IFNAME|)
```

Parameters

(IFNAME|)	Clears information only of this interface.

Command Mode

Exec Mode and Privileged Exec mode

Applicability

This command was introduced before OcNOSversion7.0.0.

Examples

```
OcNOS#show lldp neighbors

Loc PortID        Rem Host Name         Rem Chassis Id
Rem Port Name      Rem Port Id                              Agent Mode
-------------------------------------------------------------------------------
-------------------------------------------------------------------------
eth0              VN48KYC0C5            34c5.15b9.c740
20                  20                                     Nearest bridge
ce5               OcNOS                 5c07.5828.4fb0
ce5                 5c07.5828.4fb5                         Nearest bridge

OcNOS#clear lldp neighbors

OcNOS#show lldp neighbors

Loc PortID        Rem Host Name         Rem Chassis Id
Rem Port Name      Rem Port Id                              Agent Mode
-------------------------------------------------------------------------------
-------------------------------------------------------------------------
```

lldp-agent

Use this command to create an LLDP agent mode.

Note: This command is not supported in SVLAN, VLAN, and loopback interfaces.

Use the `no` parameter to remove configured lldp agent mode.

Command Syntax

```
lldp-agent (non-tpmr-bridge |customer-bridge| )
no lldp-agent (non-tpmr-bridge |customer-bridge| )
```

Parameters

`non-tpmr-bridge`

non-tpmr-bridge

`customer-bridge`

customer-bridge

Default

By default LLDP agent is disabled.

Command Mode

Interface Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent customer-bridge
(if-lldp-agent)#

(if-lldp-agent)#no lldp-agent customer-bridge
(if-lldp-agent)#exit
(config-if)#
```

debug lldp

Use this command to set the debugging functions for LLDP.

Use the no form of this command to turn off LLDP debugging functions

Command Syntax

```
debug lldp (event|ha|rx|tx|message)
no debug lldp (event|ha|rx|tx|message)
```

Parameters

`event`	Enable or disable event debugging
`ha`	Enable or disable high availability debugging
`rx`	Enable or disable RX debugging
`tx`	Enable or disable TX debugging
`message`	Enable or disable NSM message debugging

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug lldp event
#debug lldp message
```

lldp run

Use this command to start the Link Layer Discovery Protocol (LLDP)

Use the no form of this command to stop LLDP

Command Syntax

```
lldp run
no lldp run
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#lldp run

(config)#no lldp run
```

lldp tlv basic-mgmt

Use this command to select and unselect basic management TLVs in LLDP frames at the interface agent level. This command has precedence over the global configurations for inclusion of TLVs in LLDP frames.

Use the `no` parameter to remove the basic management TLV select/unselect configuration from the interface agent level.

Command Syntax

```
lldp tlv basic-mgmt (management-address|port-description|system-
  capabilities|system-description|system-name) (select|unselect)
no lldp tlv basic-mgmt (management-address|port-description|system-
  capabilities|system-description|system-name)
```

Parameters

`management-address`	Management address TLV
`port-description`	Port description TLV
`system-capabilities`	System capabilities TLV
`system-description`	System Description TLV
`system-name`	System name TLV
`select`	Select the LLDP TLV to send
`unselect`	Unselect the LLDP TLV to send

Default Value

None

Command Mode

LLDP agent mode

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)lldp-agent
(if-lldp-agent)#lldp tlv basic-mgmt system-name select
(if-lldp-agent)#exit
```

lldp tlv med

Use this command to select and unselect Media Endpoint Devices (MED) TLVs in LLDP frames at the interface agent level. This command has precedence over the global configurations for inclusion of TLVs in LLDP frames.

LLDP MED TLVs determine the capabilities the connected device supports and the capabilities the device has enabled.

Use the `no` parameter to remove the MED TLV select/unselect configuration from the interface agent level.

Command Syntax

```
lldp tlv med (network-policy|location|inventory|media-capabilities|extended-power-via-mdi) (select|unselect)
no lldp tlv med (network-policy|location|inventory|media-capabilities|extended-power-via-mdi)
```

Parameters

`network-policy`	Network-policy TLV
`location`	Location TLV
`inventory`	Inventory TLV
`media-capabilities`	Media-capabilities TLV
`extended-power-via-mdi`	Extended-power-via-mdi TLV (when PoE is available)
`select`	Select the LLDP TLV to send
`unselect`	Unselect the LLDP TLV to send

Default Value

None

Command Mode

LLDP agent mode

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)lldp-agent
(if-lldp-agent)#lldp tlv med network-policy select
(if-lldp-agent)#exit
```

lldp tlv ieee-8021-org-specific

Use this command to select and unselect ieee-8021-org-specific TLVs in LLDP frames at the interface agent level. This command has precedence over the global configurations for inclusion of TLVs in LLDP frames.

Use the `no` parameter to remove the ieee-8021-org-specific TLV select/unselect configuration from the interface agent level.

Command Syntax

```
lldp tlv ieee-8021-org-specific (link-agg|mgmt-vid|port-ptcl-vlanid|port-
  vlanid|ptcl-identity|vid-digest|vlan-name) (select|unselect)
no lldp tlv ieee-8021-org-specific {port-vlanid| port-ptcl-vlanid| vlan-name|ptcl-
  identity|vid-digest|mgmt-vid|link-agg}
```

Parameters

`link-agg`	Link-aggregation TLV
`mgmt-vid`	Management VLAN identifier TLV
`port-ptcl-vlanid`	Port protocol VLAN identifier TLV
`port-vlanid`	Port VLAN identifier TLV
`ptcl-identity`	Protocol-identifier TLV
`vid-digest`	VLAN identifier digest TLV
`vlan-name`	VLAN name TLV
`select`	Select the LLDP TLV to send
`unselect`	Unselect the LLDP TLV to send

Default Value

None

Command Mode

LLDP agent mode

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)lldp-agent
(if-lldp-agent)#lldp tlv ieee-8021-org-specific port-vlanid select
(if-lldp-agent)#exit
```

lldp tlv ieee-8023-org-specific

Use this command to select and unselect ieee-8023-org-specific TLVs in LLDP frames at the interface agent level. This command has precedence over the global configurations for inclusion of TLVs in LLDP frames.

Use the `no` parameter to remove the ieee-8023-org-specific TLV select/unselect configuration from the interface agent level.

Command Syntax

```
lldp tlv ieee-8023-org-specific (mac-phy| power-via-mdi| max-mtu-size)
  (select|unselect)
no lldp tlv ieee-8023-org-specific (mac-phy| power-via-mdi| max-mtu-size)
```

Parameters

`mac-phy`	Provider edge port VLAN ID TLV
`power-via-mdi`	Power-via-MDI TLV (when PoE is available)
`max-mtu-size`	Maximum MTU size TLV
`select`	Select the LLDP TLV to send
`unselect`	Unselect the LLDP TLV to send

Default Value

None

Command Mode

LLDP agent mode

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)lldp-agent
(if-lldp-agent)#lldp tlv ieee-8023-org-specific mac-phy select
(if-lldp-agent)#exit
```

lldp tlv-select basic-mgmt

Use this command to select basic management TLVs to be include in the LLDP frames.

Use the `no` parameter to disable basic management TLVs.

Command Syntax

```
lldp tlv-select basic-mgmt (management-address|port-description|system-
  capabilities|system-description|system-name)
no lldp tlv-select basic-mgmt (management-address|port-description|system-
  capabilities|system-description|system-name)
```

Parameters

`management-address`
: Management address specific TLV

`port-description`
: Port description specific TLV

`system-capabilities`
: System capabilities specific TLV

`system-description`
: System Description specific TLV

`system-name`
: System name specific TLV

Default Value

None

Command Mode

Configuration mode

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#lldp tlv-select basic-mgmt system-name
```

lldp tlv-select ieee-8021-org-specific

Use this command to select ieee-8021-org-specific TLVs to include in the LLDP frames.

Use the `no` parameter to disable ieee-8021-org-specific TLVs.

Command Syntax

```
lldp tlv-select ieee-8021-org-specific (link-agg|mgmt-vid|port-ptcl-vlanid|port-vlanid|ptcl-identity|vid-digest|vlan-name)
no lldp tlv-select ieee-8021-org-specific {port-vlanid| port-ptcl-vlanid| vlan-name|ptcl-identity| vid-digest|mgmt-vid|link-agg}
```

Parameters

`link-agg`	Link-aggregation TLV
`mgmt-vid`	Management VLAN identifier TLV
`port-ptcl-vlanid`	Port protocol VLAN identifier TLV
`port-vlanid`	Port VLAN identifier TLV
`ptcl-identity`	Protocol-identifier TLV
`vid-digest`	VLAN identifier digest TLV
`vlan-name`	VLAN name TLV

Default Value

None

Command Mode

Configuration mode

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#lldp tlv-select ieee-8021-org-specific port-vlanid
```

lldp tlv-select ieee-8023-org-specific

Use this command to select ieee-8023-org-specific TLVs to be include in LLDP frames.

Use the `no` parameter to disable ieee-8023-org-specific TLVs.

Command Syntax

```
lldp tlv-select ieee-8023-org-specific (mac-phy| power-via-mdi| max-mtu-size)
no lldp tlv-select ieee-8023-org-specific (mac-phy| power-via-mdi| max-mtu-size)
```

Parameters

`mac-phy`	VLAN ID Of the provider edge port <2-4094>.
`power-via-mdi`	Power-via-MDI (only when PoE feature is available)
`max-mtu-size`	Maximum MTU size TLV

Default Value

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#lldp tlv-select ieee-8023-org-specific mac-phy
```

set lldp agt-circuit-id

Use this command to configure LLDP agt-circuit-id.

Command Syntax

```
set lldp agt-circuit-id  VALUE
```

Parameters

VALUE	Specify LLDP global agt-circuit ID.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth0
(config-if)#set lldp agt-circuit-id sample
```

set lldp chassis-id-tlv

Use this command to set the chassis ID subtype for the LLDP agent on a port.

Use `no` form of this command to unset the chassis ID subtype.

In Configure mode, the command is applied globally to all supported interfaces.

LLDP Agent mode or Interface mode has priority over the Configure mode command.

Command Syntax

```
set lldp chassis-id-tlv (if-alias | ip-address | mac-address | if-name | locally-
  assigned | ipv6-address)
no set lldp chassis-id-tlv
```

Parameters

`mac-address`	Use the MAC address as the chassis ID.
`ip-address`	Use the management IP address as the chassis ID.
`if-alias`	Use the interface description as the chassis ID.
`if-name`	Use the interface name as the chassis ID.
`locally-assigned`	Use the locally assigned value as the chassis ID.
`ipv6-address`	Use the management IPv6 address as the chassis ID.

Command Mode

LLDP Agent mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Global support in Command mode was introduced in OcNOS version 6.6.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp chassis-id-tlv ip-address
(if-lldp-agent)#no set lldp chassis-id-tlv
```

set lldp chassis locally-assigned

Use this command to set the locally assigned chassis name for the LLDP interface.

Command Syntax

```
set lldp chassis locally-assigned NAME
```

Parameters

NAME	Name assigned to the chassis.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#set lldp chassis locally-assigned box1
```

set lldp disable

Use this command to disable the admin status of a LLDP agent on a port.

Use the `no` form of this command to unset the admin status.

Command Syntax

```
set lldp disable
```

```
no set lldp disable
```

Parameters

None

Command Mode

LLDP Agent mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp disable
(if-lldp-agent)#no set lldp disable
(if-lldp-agent)#exit
```

set lldp enable

Use this command to set the admin status of a LLDP agent on a port.

Use the `no` form of this command to unset the admin status.

In Configure mode, the command is applied globally to all supported interfaces.

LLDP Agent mode or Interface mode has priority over the Configure mode command.

Command Syntax

```
set lldp enable (txonly|rxtx|rxonly)
no set lldp enable (txonly|rxtx|rxonly)
```

Parameters

`rxonly`	Receive-only
`txonly`	Transmit-only
`txrx`	Transmit and receive

Default

By default, no LLDP agent is enabled for a port.

Command Mode

LLDP Agent mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3. The `no` form CLI is introduced in OcNOS version 6.6.0.

Global support in Command mode was introduced in OcNOS version 6.6.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp enable rxonly
(if-lldp-agent)#no set lldp enable rxonly
(if-lldp-agent)#exit
```

set lldp locally-assigned

Use this command to set the locally assigned name for LLDP interface.

Use no form of this command to remove the locally assigned name for LLDP interface.

Command Syntax

```
set lldp locally-assigned NAME
no set lldp locally-assigned NAME
```

Parameters

NAME	Name assigned to the port.

Command Mode

Interface Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp locally-assigned port1
(config-if)#no set lldp locally-assigned
```

set lldp management-address-tlv

Use this command to set the sub type of the Management Address TLV.

Use `no` form of this command to unset the sub type of the Management Address TLV.

In Configure mode, the command is applied globally to all supported interfaces.

LLDP Agent mode or Interface mode has priority over the Configure mode command.

Command Syntax

```
set lldp management-address-tlv (mac-address | ip-address | ipv6-address)
no set lldp management-address-tlv
```

Parameters

`mac-address`	Use the MAC address as the Management Address.
`ip-address`	Use the management IP address as the Management Address.
`ipv6-address`	Use the management IP address as the Management Address.

Command Mode

LLDP Agent mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Global support in Command mode was introduced in OcNOS version 6.6.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp management-address-tlv ip-address
(if-lldp-agent)#no set lldp management-address-tlv
```

set lldp med-devtype

Use this command to configure the LLDP device type as Network-Connectivity/ End-Point Class1/ End-Point Class2/ End-Point Class3 device.

Use the `no` parameter to un set the configured LLDP device type.

Command Syntax

```
set lldp med-devtype (net-connect| ep-class1| ep-class2| ep-class3)
no lldp med-devtype (net-connect| ep-class1| ep-class2| ep-class3)
```

Parameters

`net-connect`	Set device type as Network-Connectivity
`ep-class1`	Set device type as End-Point Class1
`ep-class2`	Set device type as End-Point Class2
`ep-class3`	Set device type as End-Point Class3

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp med-devtype ep-class1
(config-if)#exit

#configure terminal
(config)#interface eth0
(config-if)#no set lldp med-devtype
(config-if)#exit
```

set lldp msg-tx-hold

Use this command to set the `msg-tx-hold` parameter that determines the Time To Live (TTL) value for LLDPDUs to be transmitted by the port. The value set with this command is multiplied by the `lldp timer msg-tx-interval` value, which determines the final TTL value.

Use `no` form of this command to set the default value of message transmit hold.

In Configure mode, the command is applied globally to all supported interfaces.

LLDP Agent mode or Interface mode has priority over the Configure mode command.

Command Syntax

```
set lldp msg-tx-hold <1-100>
no set lldp msg-tx-hold
```

Parameters

`<1-100>`	Time in seconds to set message transmit hold.

Default

The default value of message transmit hold is 4 seconds.

Command Mode

LLDP agent mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Global support in Command mode was introduced in OcNOS version 6.6.0.

Examples

```
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp msg-tx-hold 3
(if-lldp-agent)#no set lldp msg-tx-hold
```

set lldp port-id-tlv

Use this command to set the sub type of the Port ID.

Use `no` form of this command to unset the sub type of the Port ID.

In Configure mode, the command is applied globally to all supported interfaces.

LLDP Agent mode or Interface mode has priority over the Configure mode command.

Command Syntax

```
set lldp port-id-tlv (if-alias | ip-address | mac-address | if-name | agt-circuit-
  id | locally-assigned | ipv6-address)
no set lldp port-id-tlv
```

Parameters

`mac-address`	Use the MAC address as the port-id-tlv.
`ip-address`	Use the management IP address as the port-id-tlv
`if-alias`	Use the IP alias as the port-id-tlv
`if-name`	Use the interface name as the port-id-tlv
`agt-circuit-id`	Use the agt-circuit-id name as the port-id-tlv
`locally-assigned`	Use the locally assigned value as the port-id-tlv
`ipv6-address`	Use the management IP address as the port-id-tlv

Command Mode

LLDP Agent mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Global support in Command mode was introduced in OcNOS version 6.6.0.

Examples

```
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp port-id-tlv ip-address
(if-lldp-agent)#no set lldp port-id-tlv
```

set lldp timer

Use this command to set the interval at which LLDP frames are transmitted.

Use `no` form of this command to set the default value for timer.

In Configure mode, the command is applied globally to all supported interfaces.

LLDP Agent mode or Interface mode has priority over the Configure mode command.

Command Syntax

```
set lldp timer msg-fast-tx <1-3600>
set lldp timer msg-tx-interval <5-3600>
set lldp timer reinit-delay <1-10>
no set lldp timer msg-fast-tx
no set lldp timer msg-tx-interval
no set lldp timer reinit-delay
```

Parameters

`msg-fast-tx`	Set the value in range <1-3600>
`msg-tx-interval`	Set the value in range <5-3600>
`reinit-delay`	Set the value in range <1-10>

Default Values

The default value for `msg-fast-tx` is 1 second.

The default value for `msg-tx-interval` is 30 seconds.

The default value for `reinit-delay` is 2 seconds.

Command Mode

LLDP Agent mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Global support in Command mode was introduced in OcNOS version 6.6.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp timer msg-fast-tx 40
(if-lldp-agent)#no set lldp timer msg-fast-tx
(if-lldp-agent)#exit

#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
```

```
(if-lldp-agent)#set lldp timer msg-tx-interval 40
(if-lldp-agent)#no set lldp timer msg-tx-interval
(if-lldp-agent)#exit

#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp timer reinitDelay 3
(if-lldp-agent)#no set lldp timer reinitDelay
(if-lldp-agent)#exit
```

set lldp too-many-neighbors

Use this command to set the action to take when the remote table is full.

Use no form of this command to unset too many neighbors parameters.

In Configure mode, the command is applied globally to all supported interfaces.

LLDP Agent mode or Interface mode has priority over the Configure mode command.

Command Syntax

```
set lldp too-many-neighbors limit <1-65535> discard received-info timer <1-65535>
set lldp too-many-neighbors limit <1-65535> discard existing-info MAC timer <1-
  65535>
no set lldp too-many-neighbors limit
```

Parameters

`limit`	The limit on the number of LLDP neighbors.
`<1-65535>`	Upper limit for the number of Remote LLDP Information.
`received-info`	The information received for this neighbor.
`timer`	The period after which received information is discarded.
`<1-65535>`	The period in seconds after which received information is discarded.
`existing-info`	The information for this neighbor.
`MAC`	Identifies the remote LLDP Agent for which information is discarded.
`timer`	The period in seconds after which existing information is discarded.
`<1-65535>`	The period in seconds after which existing information is discarded.

Default Value

No upper limit is enforced for the number of remote LLDP agents.

Command Mode

LLDP Agent mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Global support in Command mode was introduced in OcNOS version 6.6.0.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#lldp-agent
(if-lldp-agent)#set lldp too-many-neighbors limit 20 disc existing-info
1001.1001.1001 timer 1

(config)#interface eth1
```

```
(config-if)#lldp-agent
(if-lldp-agent)#set lldp too-many-neighbors limit 1 discard received-info
timer 1
```

set lldp tx-fast-init

Use this command to determine the maximum value of LLDP frames that are transmitted during a fast transmission period.

Use `no` form of this command to set fast transmission period to default value.

In Configure mode, the command is applied globally to all supported interfaces.

LLDP Agent mode or Interface mode has priority over the Configure mode command.

Command Syntax

```
set lldp tx-fast-init <1-8>
no set lldp tx-fast-init
```

Parameters

`tx-fast-init`	Set the message transmit interval value <1-8>.

Default Value

Default value is 4.

Command Mode

LLDP Agent mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Global support in Command mode was introduced in OcNOS version 6.6.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#lldp-agent
(if-lldp-agent)#set lldp tx-fast-init 4
(if-lldp-agent)#no set lldp tx-fast-init
(if-lldp-agent)#exit
```

set lldp tx-max-credit

Use this command to set the maximum value of transmission credit, which signifies the number of consecutive LLDP frames transmitted.

Use `no` form of this command to set the maximum value of transmission credit to default value.

In Configure mode, the command is applied globally to all supported interfaces.

LLDP Agent mode or Interface mode has priority over the Configure mode command.

Command Syntax

```
set lldp tx-max-credit <1-10>
no set lldp tx-max-credit
```

Parameters

`tx-max-credit`	The maximum value of transmission credit.

Default Value

Default value is 5

Command Mode

LLDP Agent mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Global support in Command mode was introduced in OcNOS version 6.6.0.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)lldp-agent
(if-lldp-agent)#set lldp tx-max-credit <1-10>
(if-lldp-agent)#no set lldp tx-max-credit
(if-lldp-agent)#exit
```

show debugging lldp

Use this command to display LLDP debugging information.

Command Syntax

```
show debugging lldp
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following sample output displays information about an LLDP debugging.

```
#show debugging lldp
LLDP debugging status:
 LLDP message debugging is on
```

show lldp neighbors

Use this command to display LLDP neighbors information.

Command Syntax

```
show lldp (nearest-bridge| non-tpmr-bridge| customer-bridge|) neighbors
  (brief|details)
```

Parameters

`nearest-bridge`	Display LLDP nearest bridge information
`non-tpmr-bridge`	Display LLDP non-TPMR-bridge information
`customer-bridge`	Display LLDP customer-bridge information
`neighbor`	Neighbor
`brief`	Brief
`details`	Details

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.1.

Example

The following sample output displays information about an LLDP neighbors

```
#sh lldp nearest-bridgr neighbors brief
Loc PortID  Rem Host Name   Rem Chassis Id  Rem Port Id   Agent Mode

-------------------------------------------------------------------------------
xe3/1        OcNOS       ecf4.bbfe.2864  ecf4.bbb2.4c65 Nearest bridge


#show lldp neighbors detail

-------------------------------------------------------------------------------
Nearest bridge Neighbors
 Interface Name : xe11
 Mandatory TLVs
 Chassis id type : MAC address [8cea.1b67.236c]
 Port id type : MAC address [8cea.1b28.4f6d]
 Time to live : 121
 Basic Management TLVs
 System Name : OcNOS
 System Description : Hardware Model:EC_AS5912-54X, Software version: OcNOS,1.3.1.122
 Port Description : xe11
 Remote System Capabilities : Bridge Router
 Capabilities Enabled : Router
```

```
Management Address : MAC Address [8cea.1b67.236c]
Interface Number subtype : ifindex
Interface Number : 10011
OID Number : 0
802.1 Org specific TLVs
Port vlan id : 0
Port & Protocol vlan id : 0
Remote Configured VLANs : None
Remote Protocols Advertised: None
Remote VID Usage Digest : 0
Remote Management Vlan : 0
Link Aggregation Capability: capable of being aggregated
Link Aggregation Status : not currently in aggregation
Link Aggregation Port ID :
802.3 Org specific TLVs
AutoNego Support : Supported
AutoNego Status : Disabled
AutoNego Capability : 16
Operational MAU Type : 54 [Four-pair Category 6A or better, full duplex mode only]
Max Frame Size : 1518
```

Table 1-8 Shows the output details.

Table 1-7: show lldp neighbor output details

Entry	Description
Loc Port ID	Local interface SNMP index (appears when the interface option is used).
Rem Host Name	Name of the remote host.
Rem Chassis Id	Remote chassis identifier of the chassis type listed.
Rem Port Id	Remote port identifier of the port type listed.
Agent Mode	Agent mode enabled to the nearest bridge.
Time to live	Number of seconds for which this information is valid.
Interface Name	Name of the interface.
Chassis id type	Chassis identifier of the chassis type listed.
Port id type	Type of port identifier supplied, such as Locally assigned.
System Name	Name supplied by the system on the interface.
System Description	Description supplied by the system on the interface.
Port Description	The port description field uses the configured port description, the port name or the SNMP if Index (appears when the interface option is used).
Remote System Capabilities	Remote system capabilities (such as Bridge, Bridge Router, and Bridge Telephone) that are supported.

Table 1-7: show lldp neighbor output details

Entry	Description
Capabilities Enabled	Enabled by the system on the interface (appears when the interface option is used).
Management Address	Details of management address (such as 10.204.35.34).
Interface Number subtype	Interfaces subtype for which neighbor information is available.
Interface Number	Interfaces for which neighbor information is available.
OID Number	Number of identifier.
Port VLAN ID	Details of the port VLAN identifier.
Protocol VLAN ID	Details of the protocol VLAN identifier.
Remote Configured VLANs	Details of the remote configured VLAN.
Remote Protocols Advertised	Details of the remote protocols.
Remote VID usage Digest	Details of the VID usage.
Remote Management VLAN	Details of the management VLAN.
Link Aggregation Capability	Capabilities that supported by the link aggregation on the interface.
Link Aggregation Status	Status of the link aggregation.
Link Aggregation Port ID	Details of the link aggregation port identifier.
Auto Nego Support	Support of the auto nego on the interface.
Auto Nego Status	Status of the auto nego.
Auto Nego Capability	Capabilities that supported by the auto nego on the interface.
Operational MAU Type	Type of operational MAU on the interface.
Max Frame Size	Maximum frame size on the transit.

show lldp interface

Use this command to display LLDP interface information.

Command Syntax

```
show lldp interface IFNAME (nearest-bridge| non-tpmr-bridge| customer-bridge | )
  (neighbor| )
```

Parameters

`IFNAME`

Display LLDP interface information for all agent

`nearest-bridge`

Display LLDP nearest bridge information

`non-TPMR-bridge`

Display LLDP non-TPMR-bridge information

`customer-bridge`

Display LLDP customer-bridge information

`neighbor`

Display LLDP neighbor details.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show lldp interface eth0
Agent Mode : Customer-bridge
Enable (tx/rx): N/N
MED Enabled :N
Device Type: NOT_DEFINED
LLDP Agent traffic statistics:
Total frames transmitted: 0
Total entries aged: 0
Total frames recieved: 0
Total frames received in error: 0
Total frames discarded: 0
Total discarded TLVs: 0
Total unrecognised TLVs: 0

Agent Mode : Non-TPMR-bridge
Enable (tx/rx): N/N
MED Enabled :N
Device Type: NOT_DEFINED
LLDP Agent traffic statistics:
Total frames transmitted: 0
```

```
Total entries aged: 0
Total frames recieved: 0
Total frames received in error: 0
Total frames discarded: 0
Total discarded TLVs: 0
Total unrecognised TLVs: 0

Agent Mode : Nearest bridge
Enable (tx/rx): Y/Y
MED Enabled :N
Device Type: NOT_DEFINED
LLDP Agent traffic statistics:
Total frames transmitted: 2495
Total entries aged: 0
Total frames recieved: 0
Total frames received in error: 0
Total frames discarded: 0
Total discarded TLVs: 0
Total unrecognised TLVs: 0
```

Table 1-8 Shows the output details.

Table 1-8: show lldp interface output details

Entry	Description
Agent Mode	Agent mode enabled to the customer-bridge, Non-TPMR-bridge, and nearest bridge.
Enable (tx/rx)	Enables the transmit and receive on the interface.
Device Type	Type of device in the networks.
LLDP Agent traffic statistics	Statistics on exchanged LLDP frames between a device and neighbors.
Total frames transmitted	Number of frames transmitted in network.
Total entries aged	Number of aged entries in a networks.
Total frames received	Number of frames received from the neighbor network.
Total frames received in error	Number of frames not received from the neighbor network.
Total discarded TLVs	Number of TLVs discarded in transit.
Total unrecognised TLVs	Number of unrecognised TLVs in transit.

snmp restart lldp

Use this command to restart SNMP in Link Layer Discovery Protocol (LLDP)

Command Syntax

```
snmp restart lldp
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#snmp restart lldp
```

CHAPTER 2 Provider Bridging Commands

This chapter describes the Provider Bridging (PB) commands.

IEEE 802.1ad standardizes the architecture and bridged protocols to allow Ethernet frames with multiple VLAN tags. Packets through a provider network are doubly tagged with both an:

Note: Customer-Network Port is not supported in Qumran1 series platforms.

- Inner (C-VLAN) tag which is the customer network VLAN identifier
- Outer (S-VLAN) tag which is the service provider network VLAN identifier

bridge protocol provider-mstp

Use this command to create a provider multiple spanning-tree protocol (MSTP) bridge. MSTP bridges can have different spanning-tree topologies for different VLANs inside a region of similar MSTP bridges.

Using this command creates an instance of the spanning tree, and associates the VLANs specified with that instance. A bridge created by this command forms its own separate region.

The multiple spanning tree protocol, like the rapid spanning tree protocol, provides rapid reconfiguration features, while providing load-balancing capability.

Command Syntax

```
bridge <1-32> protocol provider-mstp (edge|)
```

Parameters

`<1-32>`	Bridge identifier.
`edge`	Configure as an edge bridge.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 2 protocol provider-mstp edge
```

bridge protocol provider-rstp

Use this command to add an IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) bridge.

After creating a bridge instance, add interfaces to the bridge using the `bridge-group` command. Bring the bridge instance into operation with the `no shutdown` command in interface mode.

Command Syntax

```
bridge <1-32> protocol provider-rstp (edge|)
```

Parameters

`<1-32>`	Bridge identifier.
`edge`	Configure as an edge bridge.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 2 protocol provider-rstp edge
```

cvlan registration table

Use this command to create a customer VLAN (CVLAN) registration table that maps between CVLANs and service provider VLANs (SVLANs).

Use the `no` parameter with this command to delete the CVLAN registration table.

Command Syntax

```
cvlan registration table WORD bridge <1-32>
no cvlan registration table WORD bridge <1-32>
```

Parameters

`WORD`	Name of the CVLAN registration table.
`<1-32>`	Specify a bridge ID.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#cvlan registration table customer1
(config-cvlan-registration)#
```

cvlan svlan

Use this command to map one or more customer VLANs (CVLANs) to a service provider VLAN (SVLAN).

To update the optional QoS parameters cos-to-queue and remark-cos, execute the complete command along with the optional parameters. To remove these options, execute the same command by removing the optional parameters.

Refer `qos profile` commands from configuration guide for more details about qos profiles.

Use the `no` forms of this command to delete a mapping.

Command Syntax

```
cvlan VLAN_RANGE2 (cvlan VLAN_ID|) svlan VLAN_ID ({untagged-pep|untagged-
  cep}|)({cos-to-queue NAME | remark-cos}|)
no cvlan VLAN_RANGE2  svlan VLAN_ID
```

Parameters

`cvlan`	CVLAN
`VLAN_RANGE2`	VLAN identifier <1-4094> or range such as 2-5,10 or 2-5,7-19
`cvlan`	Translation of CVID
`VLAN_ID`	Translated CVID <1-4095>
`svlan`	SVLAN corresponding to the C-VLAN
`VLAN_ID`	VLAN identifier 1-4094>
`untagged-pep`	Provider edge port is untagged for this CVLAN
`untagged-cep`	Customer edge port is untagged for this CVLAN
`cos-to-queue`	Configure cos-to-queue map for cvlan
`NAME`	Ingress profile to modify queue/color on basis of c-cos
`remark-cos`	Remark Egress COS

Command Mode

CVLAN Registration mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS version 3.0.

Example

```
#configure terminal
(config)#cvlan registration table customer1 bridge 1
(config-cvlan-registration)#cvlan 2 svlan 3
(config-cvlan-registration)#cvlan 3 svlan 3 cos-to-queue c1 remark-cos
(config-cvlan-registration)#cvlan 100 cvlan 101 svlan 200 cos-to-queue p1
remark-cos
(config-cvlanregistration)#cvlan 3 svlan 3 remark-cos
(config-cvlan-registration)#cvlan 4 svlan 5 untagged-pep
(config-cvlan-registration)#cvlan 5 svlan 6 untagged-cep
(config-cvlan-registration)#no cvlan 3 svlan 3
```

```
(config-cvlan-registration)#cvlan 23 svlan 31 untagged-pep untagged-cep cos-
to-queue p1 remark-cos
(config-cvlan-registration)#cvlan 15-16 svlan 18 untagged-cep remark-cos
```

dot1ad ethertype

Use this command to change the TPID for a port.

Use the no form of this command to set the TPID to its default value.

Command Syntax

```
dot1ad ethertype (0x8100 | 0x88a8 | 0x9100 | 0x9200)
no dot1ad ethertype
```

Parameters

0x8100	IEEE 802.1Q VLAN-tagged frame
0x88a8	IEEE 802.1ad Provider Bridging Service VLAN tag identifier (S-Tag)
0x9100	Supported for interoperability with legacy devices
0x9200	Supported for interoperability with legacy devices

Default

The default TPID value is 8100.

Command Mode

Interface Mode

Applicability

This command was introduced before OcNOS version 3.0.

Examples

```
(config)#interface xe1
(config-if)#dot1ad ethertype 0x9100
(config-if)#exit
(config)#interface xe1
(config-if)#no dot1ad ethertype
(config-if)#exit
```

show cvlan registration table

Use this command to display the CVLAN registration table.

Command Syntax

```
show cvlan registration table (WORD|bridge <1-32>|WORD bridge <1-32>|)
```

Parameters

WORD	CVLAN registration table name.
<1-32>	Bridge identifier

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh cvlan registration table bridge 1
Bridge          Table Name       Port List
======          ==========       =========
  1               map              xe17

CVLAN ID      T-CVLAN ID     SVLAN ID     Profile Name    Egress remark-Cos
 ========    ==========     ========    ============    =================
 100             101            200          p1              Yes
```

Table 2-9 explains the output fields.

Table 2-9: show cvlan registration table output

Entry	Description
Bridge	ID number of the bridge associated with the Customer VLAN (CVLAN).
Table Name	ID of the CVLAN registration table.
Port List	List of ports used by this CVLAN (including Link aggregators).
CVLAN ID	ID number of the CVLAN.
T-CVLAN ID	Translation CVLAN ID.
SVLAN ID	ID number of the Service VLAN (SVLAN) associated with the CVLAN.
Profile Name	cos-to-queue profile name.
Egress remark-Cos	Remark Egress Cos

switchport customer-edge

Use this command to set the switching characteristics of the layer 2 interface and the default customer VLAN.

Use the `no` form of this command to remove a customer VLAN.

Command Syntax

```
switchport customer-edge (access|hybrid) vlan <1-4094>
no switchport customer-edge (access|hybrid) vlan
```

Parameters

`access`	Set the layer 2 interface as access.
`hybrid`	Set the layer 2 interface as hybrid.
`<1-4094>`	Set the default VID for the interface.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport customer-edge access vlan 3

(config)#interface eth0
(config-if)#no switchport customer-edge access vlan
```

switchport customer-edge hybrid

Use this command to set the switching characteristics of the Layer 2 customer-facing interface to hybrid. Both tagged and untagged frames will be classified over hybrid interfaces.

Command Syntax

```
switchport customer-edge hybrid allowed vlan add VLAN_ID
switchport customer-edge hybrid allowed vlan remove VLAN_ID
switchport customer-edge hybrid allowed vlan all
switchport customer-edge hybrid allowed vlan none
```

Parameters

`add`	Add a VLAN to transmit and receive through the Layer 2 interface.
`VLAN_ID`	ID of the VLAN <1-4094>.
`remove`	Remove a VLAN from the member set.
`VLAN_ID`	ID of the VLAN <1-4094>.
`all`	Allow all VLANs to transmit and receive through the Layer 2 interface.
`none`	Allow no VLANs to transmit and receive through the Layer 2 interface.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth0
(config-if)#switchport customer-edge hybrid allowed vlan add 2
```

switchport customer-edge trunk

Use this command to set the Layer2 interface as trunk.

Command Syntax

```
switchport customer-edge trunk allowed vlan add VLAN_ID
switchport customer-edge trunk allowed vlan remove VLAN_ID
switchport customer-edge trunk allowed vlan all
switchport customer-edge trunk allowed vlan none
```

Parameters

`add`	Add a VLAN to the member set.
`VLAN_ID`	Specify a VLAN ID <2-4094>
`remove`	Remove a VLAN from the member set.
`all`	Allow all VLANs to transmit and receive through the Layer 2 interface.
`none`	Allow no VLANs to transmit and receive through the Layer 2 interface.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#switchport customer-edge trunk allowed vlan add 12
```

switchport customer-edge vlan registration

Use this command to configure the VLAN registration parameters.

Use the `no` parameter with this command to delete the mapping from the interface.

Command Syntax

```
switchport customer-edge vlan registration WORD
no switchport customer-edge vlan registration
```

Parameters

`WORD`	Name of the CVLAN registration table.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#switchport customer-edge vlan registration customer1
```

switchport customer-network allowed vlan

Use this command to add SVLAN IDs to the Customer Network Port.

Note: Customer-Network Port is not supported in Qumran1 series platforms.

Command Syntax

```
switchport customer-network allowed vlan add VLAN_RANGE
```

Parameters

VLAN_RANGE	VLAN identifier <1-4094> or range such as 2-5,10 or 2-5,7-19.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 6.2.0.

Examples

In this example, the xe1 interface allows S-TAG 100-200 and 400 traffic from customer.

```
(config)#interface xe1
(config-if)#switchport
(config-if)#dot1ad ethertype 0x88a8
(config-if)#bridge-group 1
(config-if)#switchport mode customer-network
(config-if)#switchport customer-network allowed vlan add 100-200,400
```

switchport customer-network vlan

Use this command to set the default SVLAN ID for the Customer Network Port.

Note: Customer-Network Port is not supported in Qumran1 series platforms.

Command Syntax

```
switchport customer-network vlan <2-4094>
no switchport customer-network vlan
```

Parameters

<2-4094>	Set the default VLAN ID for the interface.

Default

Default Customer Network VLAN is 1.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 6.2.0

Examples

In this example, the xe1 interface allows C-TAG/untagged traffic from customers, adding SVLAN ID 100 before forwarding to the provider network. While egressing out, the SVLAN ID 100 will be stripped out.

```
(config)#interface xe1
(config-if)#switchport
(config-if)#dot1ad ethertype 0x88a8
(config-if)#bridge-group 1
(config-if)#switchport mode customer-network
(config-if)#switchport customer-network allowed vlan add 100
(config-if)#switchport customer-network vlan 100
```

switchport mode

Use this command to set the switching characteristics of the Layer 2 interface.

Note: Customer-Network Port is not supported in Qumran1 series platforms.

Command Syntax

```
switchport mode (provider-network|customer-edge|customer-network)
```

Parameters

`provider-network`	Provider network.
`customer-edge`	Customer edge.
`customer-network`	Customer network.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode provider-network
```

switchport mode customer-edge

Use this command to set the switching characteristics of the Layer 2 customer facing interface and classify only untagged frames. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Command Syntax

```
switchport mode customer-edge (access|hybrid|trunk)
```


```
switchport mode customer-edge (access|hybrid|trunk)
```


Parameters

`access`	Set the layer 2 interface as access.
`hybrid`	Set the layer 2 interface as hybrid.
`trunk`	Set the layer 2 interface as trunk.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode customer-edge access
```

switchport mode customer-edge hybrid acceptable-frame-type

Use this command to set the layer 2 interface acceptable frames types. This processing occurs after VLAN classification.

Command Syntax

```
switchport mode customer-edge hybrid acceptable-frame-type (all|vlan-tagged)
```

Parameters

`all`	Set all frames can be received.
`vlan-tagged`	Set only VLAN-tagged frames can be received.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode customer-edge hybrid acceptable-frame-type vlan-
tagged
```

switchport provider-network

Use this command to set the switching characteristics of the provider-network interface.

Command Syntax

```
switchport provider-network allowed vlan add VLAN_RANGE2
switchport provider-network allowed vlan remove VLAN_RANGE2
switchport provider-network allowed vlan except VLAN_RANGE2
switchport provider-network allowed vlan all
switchport provider-network allowed vlan none
```

Parameters

`add`	Add a VLAN to transmit and receive through the Layer 2 interface.
`VLAN_RANGE2`	VLAN ID 1-4094 or range(s): 2-5 10 or 2-5 7-20.
`remove`	Remove a VLAN from the member set.
`VLAN_RANGE2`	VLAN ID 1-4094 or range(s): 2-5 10 or 2-5 7-20.
`Except`	All VLANs except these VLANs are part of the member set.
`VLAN_RANGE2`	VLAN ID 1-4094 or range(s): 2-5 10 or 2-5 7-20.
`all`	Allow all VLANs to transmit and receive through the Layer 2 interface.
`none`	Allow no VLANs to transmit and receive through the Layer 2 interface.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth0
(config-if)#switchport provider-network allowed vlan add 2
```

switchport provider-network isolated-vlan

Use this command to attach a VLAN as an isolated VLAN for a provider network port.

Using an isolated VLAN for PNP ports on a switch can forward all frames received from the PNP port to all other PNP ports. However, if VLANs are configured to be isolated, they can traverse PNP port without sharing any of their frames.

Use the `no` form of this command to remove an isolated VLAN for a provider network port.

Command Syntax

```
switchport provider-network isolated-vlan VLAN_RANGE
no switchport provider-network isolated-vlan VLAN_RANGE
```

Parameters

`VLAN_RANGE`	VLAN identifier <2-4094> or range such as 2-5,10 or 2-5,7-19

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#configure terminal
(config)#bridge 1 protocol provider-rstp
(config)#vlan database
(config-vlan)#vlan 2-10 type service point-point bridge 1 state enable
(config-vlan)#exit
(config)#interface xe0
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport provider-network allowed vlan all
(config-if)#switchport provider-network isolated-vlan 2-10
```

switchport provider-network vlan translation

Use this command to add a translation table entry for CVLAN and SVLAN on a provider network port.

Use the `no` form of this command to delete a translation table entry for CVLAN and SVLAN on a provider network port.

Command Syntax

```
switchport provider-network vlan translation (cvlan <2-4094>| ) svlan <2-4094>
  (cvlan <2-4094> | ) svlan <2-4094>
no switchport (provider-network) vlan translation svlan VLAN_ID svlan VLAN_ID
no switchport (provider-network) vlan translation cvlan <1-4095> svlan <1-4095>
```

Parameters

`cvlan`	CVLAN to translate
`<2-4094>`	CVLAN identifier to translate
`svlan`	SVLAN to translate
`<2-4094>`	SVLAN identifier to translate
`cvlan`	Translated CVLAN
`<2-4094>`	Translated CVLAN identifier
`svlan`	Translated SVLAN
`<2-4094>`	Translated SVLAN identifier
`scos`	Class of Service in the Priority Code Point (PCP) field of the service provider tag (STAG)
`<0-7>`	Class-of-service value
`scfi`	Canonical Format Indicator in the Drop Eligible Indicator (DEI) field of the STAG
`<0-1>`	Canonical Format Indicator value
`ccos`	Class of Service in the PCP field of the customer tag (CTAG)
`<0-7>`	Class-of-service value
`ccfi`	Canonical Format Indicator in the DEI field of the CTAG
`<0-1>`	Canonical Format Indicator value

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode provider-network
(config-if)#switchport provider-network allowed vlan all
```

```
(config-if)#switchport provider-network vlan translation cvlan 2 svlan 3 cvlan
4 svlan 5
```

vlan type

This command allows you to create a single/range of VLAN's on provide/edge bridge.

Use the no form of this command to delete the VLAN.

Command Syntax

```
vlan VLAN_RANGE type customer bridge <1-32>
vlan VLAN_RANGE type customer bridge <1-32> name WORD
vlan VLAN_RANGE type customer bridge <1-32> state (enable | disable)
vlan VLAN_RANGE type service point-point bridge <1-32>
vlan VLAN_RANGE type service point-point bridge <1-32> name WORD
vlan VLAN_RANGE type service point-point bridge <1-32> state (enable | disable)

no vlan VLAN_RANGE type customer bridge <1-32>
no vlan VLAN_RANGE type service bridge <1-32>
```

Parameters

VLAN_RANGE	VLAN identifier <2-4094> or range such as 2-5,10 or 2-5,7-19
customer	Identifies the Customer VLAN
bridge	Specify the bridge group ID in the range <1-32>.
name	The ASCII name of the VLAN. Maximum length allowed is 16 characters.
point-point	Sets the VLAN connectivity mode to point-to-point
WORD	ASCII name of the VLAN.
state	Indicates the operational state of the VLAN.
enable	Sets VLAN into an enable state.
disable	Sets VLAN into a disable state.

Command Mode

Configuration Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)vlan 2,4,5-6 customer bridge 2
(config)vlan 10-12 service type point-point bridge 3
```

vlan type customer

Use this command to configure VLANs of type customer, to enable or disable the state of the VLANs, and to configure the name for VLANs.

Use the `no` form of this command to remove the VLAN type.

Command Syntax

```
vlan <2-4094> type customer bridge <1-32>
vlan <2-4094> type customer bridge <1-32> state (enable|disable)
vlan <2-4094> type customer bridge <1-32> name WORD
no vlan <2-4094> type customer bridge <1-32>
```

Parameters

`<2-4094>`	The VID of the VLAN that will be enabled or disabled on the bridge <2-4094>.
`type`	Identifies the VLAN as a customer, service, or VLAN.
`customer`	Identifies the Customer VLAN
`bridge`	Indicates a Service VLAN <1-32>.
`name`	The ASCII name of the VLAN. Maximum length allowed is 16 characters.
`state`	Indicates the operational state of the VLAN.
`enable`	Sets VLAN into an enable state.
`disable`	Sets VLAN into a disable state.
`WORD`	ASCII name of the VLAN.

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#vlan database
(config-vlan)#vlan 12 type customer bridge 1 name new state enable
```

CHAPTER 3 Bridge Commands

This chapter provides a description, syntax, and examples of the bridge commands. It includes the following commands:

bridge acquire

Use this command to enable a bridge to learn station location information for an instance. This helps in making forwarding decisions.

Use the `no` parameter with this command to disable learning.

Note: OcNOS supports only configuration of a single bridge.

Command Syntax

```
bridge <1-32> acquire
no bridge <1-32> acquire
```

Parameter

`<1-32>`	Bridge group ID.

Default

By default, learning is enabled for all instances.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 acquire
(config)#no bridge 3 acquire
```

bridge address

Use this command to add a static forwarding table entry for the bridge.

Use the no parameter with this command to remove the entry for the bridge

Note: Forward MAC must refer to the source MAC, and discard MAC must refer to the destination MAC.

Command Syntax

```
bridge <1-32> address XXXX.XXXX.XXXX (forward|discard) IFNAME
bridge <1-32> address XXXX.XXXX.XXXX (forward|discard) IFNAME vlan <2-4094>
bridge <1-32> address XXXX.XXXX.XXXX  (forward|discard) IFNAME vlan <2-4094> svlan
  <2-4094>
no bridge <1-32> address XXXX.XXXX.XXXX
no bridge <1-32> address XXXX.XXXX.XXXX vlan <2-4094>
no bridge <1-32> address XXXX.XXXX.XXXX vlan <2-4094> svlan <2-4094>
```

Parameters

`<1-32>`	Bridge identifier
`XXXX.XXXX.XXXX`	Media Access Control (MAC) address in HHHH.HHHH.HHHH format.
`forward`	Forward matching frames.
`discard`	Discard matching frames.
`IFNAME`	Interface on which the frame comes out.
`vlan`	Identity of the VLAN in the range of <2-4094>.
`svlan`	Identity of the SVLAN in the range of <2-4094>.

Default

By default, bridge address is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 1 address 0000.000a.0021 forward eth0
(config)#no bridge 1 address 0000.000a.0021
(config)#bridge 1 address 0011.2222.3333 forward xe5 vlan 23
(config)#no bridge 1 address 0011.2222.3333 vlan 23
(config)#bridge 1 address 0011.2222.3333 forward xe5 vlan 11 svlan 21
(config)#no bridge 1 address 0011.2222.3333 vlan 11 svlan 21
(config)#bridge 1 address 0011.2222.3334 discard xe6 vlan 12 svlan 22
(config)#no bridge 1 address 0011.2222.3334 vlan 12 svlan 22
```

bridge ageing

Use this command to specify the aging time for a learned MAC address. A learned MAC address persists until this specified time.

Note: The bridge aging time affects the ARP entries which are dependent upon the MAC addresses in hardware. If a MAC address ages out, it causes the corresponding ARP entry to refresh.

Note: On Qumran, the MAC aging time can vary by up to 16%. For example, if the MAC aging time is set to 60 seconds, the aging time can happen anywhere between 50-60 seconds.

Use the `no` form of this command to set the MAC address aging time to its default (300).

Command Syntax

```
bridge <1-32> ageing-time (0|<10-572>)
bridge <1-32> ageing disable
no bridge <1-32> ageing-time
```

Parameters

`0`	Disable Ageing Time
`<1-32>`	Bridge group ID.
`<10-572>`	Aging time in seconds.
`disable`	Turn off MAC address aging completely.

Default

By default, the aging time is 300 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 ageing-time 100
(config)#no bridge 3 ageing-time
```

bridge encapsulation dot1q

Use this command to add the TPID which is configured on a parent interface in the case of a routed packet destined to an SVI interface.

Use the `no` parameter with this command to configure the default behavior.

Note: OcNOS only supports configuration of a single bridge.

Command Syntax

```
bridge <1-32> encapsulation dot1q
no bridge <1-32> encapsulation dot1q
```

Parameter

`<1-32>`	Bridge group ID.

Default

By default, routed packets destined to an SVI interface adds 0x8100 as the outer TPID.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 4.0.

Example

```
#configure terminal
(config)#bridge 1 encapsulation dot1q
(config)#no bridge 1 encapsulation dot1q
```

bridge forward-time

Use this command to set the time (in seconds) after which (if this bridge is the root bridge) each port changes states to learning and forwarding. This value is used by all instances.

Use the `no` parameter with this command to restore the default value of 15 seconds.

Command Syntax

```
bridge <1-32> forward-time <4-30>
no bridge <1-32> forward-time
```

Parameters

`<1-32>`	Specify the bridge group ID.
`<4-30>`	Specify the forwarding time delay in seconds.

Note: Care should be exercised if the value is to be made below 7 seconds.

Default

By default, value is 15 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 forward-time 6
(config)#no bridge 3 forward-time
```

bridge hello-time

Use this command to set the hello-time, the time in seconds after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange Bridge Protocol Data Units (BPDUs). A very low value of this parameter leads to excessive traffic on the network, while a higher value delays the detection of topology change.This value is used by all instances.

Configure the bridge instance name before using this command. The allowable range of values is 1-10 seconds. However, make sure that the value of hello time is always greater than the value of hold time (2 seconds by default).

Use the `no` parameter to restore the default value of the hello time.

Note: A Bridge enforces the following relationships for Hello-time, Max-age and Forward-delay.

- 2 × (Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age
- Bridge_Max_Age >= 2 × (Bridge_Hello_Time + 1.0 seconds)

Note: Hello-time is allowed only on RSTP, IEEE and Provider-RSTP types of bridges. For MSTP and Provider-MSTP hello timer is restricted.

Command Syntax

```
bridge <1-32> hello-time <1-10>
no bridge <1-32> hello-time
```

Parameters

`<1-32>`	Specify the bridge group ID.
`<1-10>`	Specify the hello BPDU interval in seconds.

Default

By default, value is 2 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 3 hello-time 3

(config)#no bridge 3 hello-time
```

bridge max-age

Use this command to set the maximum age for a bridge. This value is used by all instances.

Maximum age is the maximum time in seconds for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. The value of maximum age should be greater than twice the value of hello time plus 1, but less than twice the value of forward delay minus 1. The allowable range for max-age is 6-40 seconds. Configure this value sufficiently high, so that a frame generated by root can be propagated to the leaf nodes without exceeding the maximum age.

Use the `no` parameter with this command to restore the default value of the maximum age.

Note: A Bridge shall enforce the following relationships for Hello-time, Max-age and Forward-delay.

- 2 × (Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age
- Bridge_Max_Age >= 2 × (Bridge_Hello_Time + 1.0 seconds)

Command Syntax

```
bridge <1-32> max-age <6-40>
no bridge <1-32> max-age
```

Parameters

`<1-32>`	Specify the bridge group ID.
`<6-40>`	Specify the maximum time, in seconds, to listen for the root bridge <6-40>.

Default

By default, bridge maximum age is 20 seconds

Command Mode

Configure Mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 max-age 12

(config)#no bridge 2 max-age
```

bridge max-hops

Use this command to specify the maximum allowed hops for a BPDU in an MST region. This parameter is used by all the instances of the MST. Specifying the maximum hops for a BPDU prevents the messages from looping indefinitely in the network. When a bridge receives an MST BPDU that has exceeded the allowed maximum hops, it discards the BPDU.

Use the `no` parameter with this command to restore the default value.

Command Syntax

```
bridge <1-32> max-hops <1-40>
no bridge <1-32> max-hops
```

Parameters

`<1-32>`	Specify the bridge-group ID.
`<1-40>`	Specify the maximum hops for which the BPDU will be valid <1-40>.

Default

By default, maximum hops in an MST region are 20

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 3 max-hops 25

#configure terminal
(config)#no bridge 3 max-hops
```

bridge priority

Use this command to set the bridge priority for the common instance. Using a lower priority indicates a greater likelihood of the bridge becoming root. The priority values can be set only in increments of 4096.

Use the `no` form of the command to reset it to the default value.

Command Syntax

```
bridge (<1-32> | ) priority <0-61440>
no bridge (<1-32> | )priority
```

Parameters

`<1-32>`	Specify the bridge group ID.
`<0-61440>`	Specify the bridge priority in the range of <0-61440>.

Default

By default, priority is 32768 (or hex 0x8000).

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 priority 4096

(config)#no bridge 2 priority
```

bridge shutdown

Use this command to disable a bridge.

Use the `no` parameter to reset the bridge.

Command Syntax

```
bridge shutdown <1-32>
bridge shutdown <1-32> ((bridge-blocked|bridge-forward)|)
no bridge shutdown <1-32>
```

Parameters

`<1-32>`	Specify the bridge group ID.
`bridge-forward`	Put all ports of the bridge into forwarding state
`bridge-blocked`	Put all ports of the bridge into blocked state

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge shutdown 4
(config)#no bridge shutdown 4
```

bridge transmit-holdcount

Use this command to set the maximum number of transmissions of BPDUs by the transmit state machine.

Use the `no` parameter with this command to restore the default transmit hold-count value.

Command Syntax

```
bridge <1-32> transmit-holdcount <1-10>
no bridge <1-32> transmit-holdcount
```

Parameters

`<1-32>`	Specify the bridge group ID.
`<1-10>`	Transmit hold-count value.

Default

By default, transmit hold-count is 6

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 transmit-holdcount 5

(config)#no bridge 1 transmit-holdcount
```

bridge-group

Use this command to bind an interface with a bridge specified by the parameter.

Use the `no` parameter with this command to disable this command.

Command Syntax

```
bridge-group (<1-32>)
no bridge-group (<1-32>)
```

Parameters

`<1-32>`	Specify the bridge group ID.

Default

By default, bridge-group is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#bridge-group 2

(config)#interface eth1
(config-if)#no bridge-group 2
```

bridge-group path-cost

Use this command to set the cost of a path associated with a bridge group. The lower the path cost, the greater the likelihood of the bridge becoming root.

Use the `no` parameter with this command to restore the default priority value.

Command Syntax

```
bridge-group <1-32> path-cost <1-200000000>
no bridge-group <1-32> path-cost
```

Parameters

`<1-32>`	Specify the bridge group ID.
`path-cost`	Specify the path-cost of a port.
`<1-200000000>`	Specify the cost to be assigned to the group.

Default

By default, bridge-group is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#bridge-group 3 path-cost 123

(config-if)#no bridge-group 3 path-cost
```

bridge-group priority

Use this command to set the port priority for a bridge. A lower priority indicates a greater likelihood of the bridge becoming root.

Command Syntax

```
bridge-group <1-32> priority <0-240>
no bridge-group <1-32> priority
```

Parameters

`<1-32>`	Specify the bridge group ID.
`<0-240>`	Specify the port priority range (a lower priority indicates greater likelihood of the interface becoming a root). The priority values can only be set in increments of 16.

Default

By default, priority is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#bridge-group 4 priority 96

(config)#interface eth1
(config-if)#no bridge-group 4 priority
```

clear allowed-ethertype

Use this command to clear statistics for each ethertype per interfaces.

```
clear allowed-ethertype statistics (IFNAME|)
```

Parameters

IFNAME	Interface name.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear allowed-ethertype statistics xe54/1

#show allowed-ethertype statistics xe54/1
Interface xe54/1
arp: 0 Packets, 0 Bytes
ipv4: 0 Packets, 0 Bytes
ipv6: 0 Packets, 0 Bytes
dropped: 0 Packets, 0 Bytes
```

clear mac address-table

Use this command to clear the filtering database for the bridge. This command can be issued to do the following:

- clear the filtering database
- clear all filtering database entries configured through CLI (static)
- clear all multicast filtering database entries
- clear all multicast filtering database entries for a given VLAN or interface
- clear all static or multicast database entries based on a mac address

Command Syntax

```
clear mac address-table (dynamic|multicast) bridge <1-32>
clear mac address-table (dynamic|multicast) (address MACADDR | interface IFNAME |
  vlan VID ) bridge <1-32>
clear mac address-table (dynamic|multicast) (address MACADDR | interface IFNAME |
  vlan VID ) (instance INST) bridge <1-32>
```

Parameters

`dynamic`	Clears all dynamic entries.
`multicast`	Clears all multicast filtering database entries.
`address`	Clear the specified MAC Address.
`MACADDR`	When filtering database, entries are cleared based on the MAC address.
`bridge`	Clears the bridge group ID. Value range is 1-32.
`bridge`	Clears the bridge group ID. Value range is 1-32.
`interface`	Clears all MAC address for the specified interface.
`bridge`	Clears the bridge group ID. Value range is 1-32.
`instance`	Clears MSTP instance ID. Value range is <1-63>.
`vlan`	Clears all MAC address for the specified VLAN. Value range is 1-4094.
`bridge`	Clears the bridge group ID. Value range is 1-32.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows how to clear multicast filtering database entries:

```
#clear mac address-table multicast bridge 1
```

This example shows how to clear multicast filtering database entries for a given VLAN.

```
#clear mac address-table multicast vlan 2 bridge 1
```

This example shows how to clear all filtering database entries learned through bridge operation for a given MAC address.

```
#clear mac address-table dynamic address 0202.0202.0202 bridge 1
```

l2protocol all learn-disable

Use this command to disable MAC address learning from all Layer 2 protocol data units (BPDUs) received on the device. When configured, the device does not learn the source MAC addresses of Layer 2 control protocol packets, including xSTP, LACP, EAP, LLDP, EFM, SyncE, and ELMI, on any interface.

Note: If the source MAC address of a Layer 2 BPDU has already been learned before this command is applied, it must be manually cleared by the user.

Use `no` form of this command to enable MAC address learning.

Command Syntax

```
l2protocol all learn-disable
no l2protocol all learn-disable
```

Parameters

None

Default

MAC address learning from Layer 2 BPDUs is enabled by default.

Command Mode

Configuration mode

Applicability

This command was introduced in OcNOS version 6.5.4.

Examples

Disable MAC learning from all Layer 2 BPDUs

```
#configure terminal
(config)#l2protocol all learn-disable
```

Re-enable MAC learning (default behavior)

```
(config)#no l2protocol all learn-disable
```

show allowed-ethertype

Use this command to show allowed and denied traffic statistics.

Note: Dropped slow protocol packets provides the count of slow protocol packets among the total dropped count. Total drop count is fetched from hardware and slow protocol packet count is fetched from software. Hence there can be one or two packet difference.

Command Syntax

```
show allowed-ethertype statistics (IFNAME|)
```

Parameters

IFNAME	Interface name.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show allowed-ethertype statistics
Interface po1
arp : 0 Packets, 0 Bytes
ipv4 : 511016709 Packets, 184897169366 Bytes
ipv6 : 0 Packets, 0 Bytes
dropped : 220 Packets, 28160 Bytes
dropped slow protocol pkts : lacp 220, efm 0, others 0
Interface xe47
arp : 0 Packets, 0 Bytes
ipv4 : 169763534 Packets, 61427990740 Bytes
ipv6 : 0 Packets, 0 Bytes
dropped : 0 Packets, 0 Bytes
Interface xe48
arp : 0 Packets, 0 Bytes
ipv4 : 0 Packets, 0 Bytes
ipv6 : 0 Packets, 0 Bytes
dropped : 0 Packets, 0 Bytes
```

show bridge

Use this command to display the filtering database for the bridge. The filtering database is used by a switch to store the MAC addresses that have been learned and which ports that MAC address was learned on.

Command Syntax

```
show bridge (ieee|rpvst+|mstp|)
```

Parameters

`ieee`	STP bridges.
`rpvst+`	RPVST+ bridges.
`mstp`	MSTP bridges.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+------------+------------------+-----+---------+
 1         1                   eth1         5254.0029.929c     1     0
 1         2                   eth1         5254.004c.dcc6     1     297
 1         1                   eth1         5254.004c.dcc6     1     291
```

Table 3-10 explains the show command output fields.

Table 3-10: show bridge output fields

Field	Description
Bridge	Bridge identifier.
VLAN, SVLAN, BVLAN	CVLAN, SVLAN, and BVLAN identifiers.
Port	Interface name.
MAC Address	Learned MAC address.
FWD	Whether frames for the MAC addresses are forwarded.
Time-out	How long the learned MAC address persists.

show interface switchport

Use this command to display the characteristics of the interface with the current VLAN.

Command Syntax

```
show interface switchport bridge <1-32>
```

Parameter

`bridge`	Bridge name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is an output of this command displaying the characteristics of this interface on bridge 2.

```
#show interface switchport bridge 2
 Interface name          : eth5
 Switchport mode         : access
 Ingress filter          : disable
 Acceptable frame types  : all
 Vid swap                : disable
 Default vlan            : 2
 Configured vlans        :    2
 Interface name          : eth4
 Switchport mode         : access
 Ingress filter          : disable
 Acceptable frame types  : all
 Vid swap                : disable
 Default vlan            : 1
 Configured vlans        :    1
```

Table 3-11 explains the show command output fields.

Table 3-11: show interface switchport output fields

Field	Description
Interface name	Display the name of interface.
Switchport mode	Port that used to connect between switches and access port.
Ingress filter	Ingress filtering examines all inbound packets and then permits or denies entry to the network.
Acceptable frame types	Type of acceptable frame in the interface.
VID swap	Displays the status of the VID swap.

Table 3-11: show interface switchport output fields (Continued)

Field	Description
Default vlan	Default value for the VLAN.
Configured vlans	Displays the information on configured VLANs.

show mac address-table count bridge

Use this command to display a count of MAC entries from the filtering database.

Command Syntax

```
show mac address-table (local|remote|) count bridge <1-32> ({(dynamic | multicast |
  static) | address MAC | interface IFNAME | vlan <1-4094> | svlan <1-4094>}|)
```

Parameter

`local`	Local dynamic FDB entries
`remote`	Remote dynamic FDB entries
`<1-32>`	Bridge group
`dynamic`	Dynamic entries
`multicast`	Multicast entries
`static`	Static entries
`MAC`	MAC address in HHHH.HHHH.HHHH format
`IFNAME`	Name of the interface
`<1-4094>`	VLAN identifier
`<1-4094>`	SVLAN identifier

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 3
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0
Total MAC Addresses in Use: 3
```

Table 3-12 explains the show command output fields.

Table 3-12: show mac address-table count output fields

Field	Description
Dynamic Address Count	Number of dynamic addresses.
Unicast MAC Address Count	Number of unicast addresses.
Multicast MAC Address Count	Number of multicast addresses.
Total MAC Addresses	Total number of addresses.

show mac address-table bridge

Use this command to display MAC entries from the filtering database.

Note: The hardware can learn the MAC address at line rate, but OcNOS will learn the MAC address at a much slower rate. The learning in OcNOS will also depend upon the current load in the system. Under normal conditions OcNOS can learn the mac-address at approximately 3000 MACs per sec.

Command Syntax

```
show mac address-table (local|remote|) bridge <1-32> ({(dynamic | multicast |
  static) | address MAC | interface IFNAME | vlan <1-4094> | svlan <1-4094>}|)
```

Parameter

`local`	Local dynamic FDB entries
`remote`	Remote dynamic FDB entries
`<1-32>`	Bridge group
`dynamic`	Dynamic entries
`multicast`	Multicast entries
`static`	Static entries
`MAC`	MAC address in HHHH.HHHH.HHHH format
`IFNAME`	Name of the interface
`<1-4094>`	VLAN identifier
`<1-4094>`	SVLAN identifier

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mac address-table bridge 1
 CVLAN  SVLAN  MAC Address       Type      Ports     Port-security
------+------+---------------+---------+---------+-------------
 100   200    1111.2222.1111  static    xe12      Disable
 102   202    1111.2222.1111  static    xe12      Disable
       201    1111.1111.1111  static    xe14      Disable
       202    1111.1111.1111  static    xe14      Disable
       203    1111.1111.1111  static    xe14      Disable
       201    0000.0700.0d00  dynamic   xe14      Disable
       202    0000.0700.0d00  dynamic   xe14      Disable
       203    0000.0700.0d00  dynamic   xe14      Disable
       204    0000.0700.0d00  dynamic   xe14      Disable
       205    0000.0700.0d00  dynamic   xe14      Disable
       206    0000.0700.0d00  dynamic   xe14      Disable
       207    0000.0700.0d00  dynamic   xe14      Disable
       208    0000.0700.0d00  dynamic   xe14      Disable
       209    0000.0700.0d00  dynamic   xe14      Disable
```

```
103    203     0000.0700.0b00  dynamic   xe12       Disable
101    201     0000.0700.0b00  dynamic   xe12       Disable
100    200     0000.0700.0b00  dynamic   xe12       Disable
102    202     0000.0700.0b00   dynamic     xe12         Disable
```

Table 3-13 explains the show command output fields.

Table 3-13: show mac address-table output fields

Field	Description
VLAN	VLAN identifier.
MAC Address	Media Access Control address.
Type	Dynamic, multicast, or static.
Ports	Interface name.

switchport

Use this command to set the mode of an interface to switched.

All interfaces are configured routed by default. To change the behavior of an interface from switched to routed, you must explicitly give the `no switchport` command.

Note: When you change the mode of an interface from switched to routed and vice-versa, all configurations for that interface are erased.

Use the `no` form of this command to set the mode to routed.

Command Syntax

```
switchport
```

```
no switchport
```

Parameters

None

Default

All interfaces are configured routed by default. To change the behavior of an interface from switched to routed, you must explicitly give the no switchport command.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport

(config)#interface eth0
(config-if)#no switchport
```

switchport allowed ethertype

Use this command to allow a set of ethertype on the access port and deny remaining traffic.

Use the no command to remove ethertype configuration.

Command Syntax

```
switchport allowed ethertype {arp|ipv4|ipv6|mpls|WORD|log}
no switchport allowed ethertype ({arp|ipv4|ipv6|mpls|WORD|log}|)
```

Parameters

`arp`	Ethertype 0x0806.
`ipv4`	Ethertype 0x0800.
`ipv6`	Ethertype 0x086dd.
`mpls`	Ethertype 0x8847.
`WORD`	Any Ethertype value (0x600 - 0xFFFF).
`log`	Log unwanted ethertype packets.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#switchport allowed ethertype arp ipv4 ipv6 log

(config-if)#no switchport allowed ethertype ipv4
```

CHAPTER 4 Spanning Tree Protocol Commands

This chapter provides a description, syntax, and examples of the Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) commands. It includes the following commands:

- debug mstp
- show debugging mstp
- show spanning-tree
- show spanning-tree mst
- show spanning-tree statistics
- spanning-tree autoedge
- spanning-tree edgeport
- spanning-tree edgeport
- spanning-tree guard
- spanning-tree instance restricted-role
- spanning-tree instance restricted-tcn
- spanning-tree link-type
- spanning-tree mst configuration
- spanning-tree restricted-domain-role
- spanning-tree restricted-role
- spanning-tree restricted-tcn
- spanning-tree te-msti configuration

bridge cisco-interoperability

Use this command to enable/disable Cisco interoperability for MSTP (Multiple Spanning Tree Protocol).

If Cisco interoperability is required, all OcNOS devices in the switched LAN must be Cisco-interoperability enabled. When OcNOS inter operates with Cisco, the only criteria used to classify a region are the region name and revision level. VLAN-to-instance mapping is not used to classify regions when interoperating with Cisco.

Command Syntax

```
bridge <1-32> cisco-interoperability (enable | disable)
```

Parameters

`<1-32>`	Specify the bridge group ID
`enable`	Enable Cisco interoperability for MSTP bridge
`disable`	Disable Cisco interoperability for MSTP bridge

Default

By default, cisco interoperability is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

To enable Cisco interoperability on a switch for a bridge:

```
#configure terminal
(config)#bridge 2 cisco-interoperability enable
```

To disable Cisco interoperability on a switch for a particular bridge:

```
#configure terminal
(config)#bridge 2 cisco-interoperability disable
```

bridge instance

Use this command to add an MST instance to a bridge.

Use the `no` form of this command to delete an MST instance identifier from a bridge.

Command Syntax

```
bridge (<1-32> | backbone) instance (<1-62>)
no bridge (<1-32> | backbone) instance (<1-62>)
```

Parameters

`<1-32>`	Bridge identifier.
`backbone`	Backbone bridge.
`<1-62>`	MST instance identifier.

Default

The bridge instance default is 1.

Command Mode

MST configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 4 protocol mstp
(config)#spanning-tree mst configuration
(config-mst)#bridge 4 instance 3
...
(config-mst)#no bridge 4 instance 3
```

bridge instance priority

Use this command to set the bridge instance priority.

Use the `no` form of this command to reset the priority to its default.

Command Syntax

```
bridge (<1-32> | backbone) instance <1-63> priority <0-61440>
no bridge (<1-32> | backbone) instance <1-63> priority
```

Parameters

`<1-32>`	Specify the bridge identifier.
`backbone`	Specifies the backbone bridge.
`<1-63>`	Specify the instance identifier.
`priority`	Specify the bridge priority for the instance. The lower the priority of the bridge, the better the chances is of the bridge becoming a root bridge or a designated bridge for the LAN. The priority values can be set only in increments of 4096. The default value is 32768.
`<0-61440>`	Specify the bridge priority.

Default

By default, bridge instance priority is 32768

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#bridge 4 instance 3 priority 1
```

bridge instance vlan

Use this command to simultaneously add multiple VLANs for the corresponding instance of a bridge.The VLANs must be created before being associated with an MST instance (MSTI). If the VLAN range is not specified, the MSTI will not be created.

Use the `no` form of this command to simultaneously remove multiple VLANs for the corresponding instance of a bridge.

Command Syntax

```
bridge (<1-32> | backbone) instance (<1-63>) vlan VLANID
no bridge (<1-32> | backbone) instance (<1-63>) vlan VLANID
```

Parameters

`<1-32>`	Bridge identifier.
`backbone`	Backbone bridge.
`<1-63>`	MST instance identifier.
`VLANID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list. For a VLAN range, specify two VLAN identifiers: the lowest and then the highest separated by a hyphen. For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces between the hyphens or commas.

Default

The bridge instance VLAN ID Interfaces default-switch is VLAN100 100 ae0.0 ae1.0 ae2.0.

Command Mode

MST configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

To associate multiple VLANs, in this case VLANs 10 and 20 to instance 1 of bridge 1:

```
#configure terminal
(config)#bridge 1 protocol mstp
(config)#spanning-tree mst configuration
(config-mst)#bridge 1 instance 1 vlan 10,20
```

To associate multiple VLANs, in this case, VLANs 10, 11, 12, 13, 14, and 15 to instance 1 of bridge 1:

```
#configure terminal
(config)#bridge 1 protocol mstp
(config)#spanning-tree mst configuration
(config-mst)#bridge 1 instance 1 vlan 10-15
```

To delete multiple VLANs, in this case, VLANs 10 and 11 from instance 1 of bridge 1:

```
#configure terminal
(config)#bridge 1 protocol mstp
(config)#spanning-tree mst configuration
```

```
(config-mst)#no bridge 1 instance 1 vlan 10,11
```

bridge multiple-spanning-tree

Use this command to enable MSTP on a bridge.

Use the `no` form of this command to disable MSTP on the bridge.

Command Syntax

```
bridge <1-32> multiple-spanning-tree enable
no bridge <1-32> multiple-spanning-tree enable (bridge-forward|bridge-block)
```

Parameters

`<1-32>`	Specify the bridge-group ID.
`enable`	Enables the spanning tree protocol.
`bridge-forward`	Puts all ports of the specified bridge into forwarding state.
`bridge-block`	Puts all ports of the specified bridge into blocking state.

Default

If the bridge-forward option is entered when using the `no` parameter, the default behavior is to put all bridge ports in forwarding state.

If the bridge-block option is entered when using the no parameter, the behavior is to put all bridge ports in blocking state.

If no options are defined after the command `no bridge <1-32> multiple-spanning-tree enable`, then the default behavior is same as `bridge-block` command.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 multiple-spanning-tree enable

#configure terminal
(config)#no bridge 2 multiple-spanning-tree enable bridge-forward
```

bridge protocol ieee

Use this command to add a IEEE 802.1d Spanning Tree Protocol bridge.

After creating a bridge instance, add interfaces to the bridge using the `bridge-group` command. Bring the bridge instance into operation with the `no shutdown` command in interface mode.

Use the `no` parameter with this command to remove the bridge.

Command Syntax

```
bridge <1-32> protocol ieee (vlan-bridge|)
no bridge <1-32>
```

Parameters

`<1-32>`	Specify the bridge group ID.
`vlan-bridge`	Specify this as a VLAN-aware bridge.

Default

Disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 protocol ieee

(config)#bridge 4 protocol ieee vlan-bridge
```

bridge protocol mstp

Use this command to create a multiple spanning-tree protocol (MSTP) bridge of a specified parameter. This command creates an instance of the spanning tree and associates the VLANs specified with that instance.

The MSTP bridges can have different spanning-tree topologies for different VLANs inside a region of “similar” MSTP bridges. The multiple spanning tree protocol, like the rapid spanning tree protocol, provides rapid reconfiguration capability, while providing load balancing ability. A bridge created with this command forms its own separate region unless it is added explicitly to a region using the `region name` command.

Use the `no` parameter with this command to remove the bridge.

Command Syntax

```
bridge <1-32> protocol mstp
no bridge <1-32>
```

Parameters

`<1-32>`	Specify the bridge group ID.

Default

Disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 protocol mstp
```

bridge protocol rstp

Use this command to add an IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) bridge.

After creating a bridge instance, add interfaces to the bridge using the `bridge-group` command. Bring the bridge instance into operation with the `no shutdown` command in Interface mode.

Use the `no` parameter with this command to remove the bridge.

Command Syntax

```
bridge <1-32> protocol rstp
bridge <1-32> protocol rstp (vlan-bridge|)
no bridge <1-32>
```

Parameters

`<1-32>`	Specify the bridge group ID.
`vlan-bridge`	(Optional) Adds a VLAN-aware bridge.

Default

Disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 protocol rstp
```

bridge rapid-spanning-tree

Use this command to enable or disable RSTP on a specific bridge. Use the `bridge-forward` option with the `no` form of the command to place all ports on the specified bridge into the forwarding state.

Use the `no` form of the command to disable the Rapid Spanning Tree protocol on a bridge.

Command Syntax

```
bridge <1-32> rapid-spanning-tree enable
no bridge <1-32> rapid-spanning-tree enable (bridge-forward|bridge-block)
```

Parameters

`<1-32>`	Specify the bridge group ID.
`enable`	Enables the spanning tree protocol.
`bridge-forward`	(Optional) Puts all ports of the specified bridge into forwarding state.
`bridge-block`	(Optional) Puts all ports of the specified bridge into blocking state.

Default

When the `bridge-forward` option is used with the `no` parameter, the default behavior puts all bridge ports in the forwarding state.

If the bridge-block option is entered when using the no parameter, the behavior is to put all bridge ports in blocking state.

If no options are defined after the command `no bridge <1-32> rapid-spanning-tree enable`, then the default behavior is same as `bridge-block` command.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
 configure terminal
(config)#bridge 2 rapid-spanning-tree enable

 configure terminal
(config)#no bridge 2 rapid-spanning-tree enable bridge-forward
```

bridge region

Use this command to create an MST region and specify its name. MST bridges of a region form different spanning trees for different VLANs.

Use the `no` form of the command to disable the Rapid Spanning Tree protocol on a region.

Command Syntax

```
bridge <1-32> region REGION_NAME
no bridge <1-32> region
```

Parameters

`<1-32>`	Specify the bridge group ID.
`REGION_NAME`	Specify the name of the region.

Default

By default, each MST bridge starts with the region name as its bridge address. This means each MST bridge is a region by itself, unless specifically added to one.

Command Mode

MST configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#bridge 3 region myRegion

(config)#spanning-tree mst configuration
(config-mst)#no bridge 3 region
```

bridge revision

Use this command to specify the number for configuration information.

Command Syntax

```
bridge <1-32> revision <0-65535>
```

Parameters

<1-32>	Specify the bridge group ID in the range of <1-32>.
<0-65535>	Specify a revision number in the range of <0-65535>.

Default

By default, revision number is 0

Command Mode

MST configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#bridge 3 revision 25
```

bridge spanning-tree

Use this command to enable the Spanning Tree Protocol on a bridge.

Use the `no` parameter to disable the Spanning Tree Protocol on the bridge.

Command Syntax

```
bridge <1-32> spanning-tree enable
no bridge <1-32> spanning-tree enable (bridge-forward|bridge-block)
```

Parameters

`<1-32>`	Specify the bridge group ID.
`enable`	Enables the spanning tree protocol on this bridge.
`bridge-forward`	Puts all ports of the specified bridge into the forwarding state.
`bridge-block`	Puts all ports of the specified bridge into the blocking state.

Default

If the bridge-forward option is entered when using the `no` parameter, the default behavior is to put all bridge ports in forwarding state.

If the bridge-block option is entered when using the no parameter, the behavior is to put all bridge ports in blocking state.

If no options are defined after the command `no bridge <1-32> spanning-tree enable`, then the default behavior is same as `bridge-block` command.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 spanning-tree enable

#configure terminal
(config)#no bridge 2 spanning-tree enable bridge-forward
```

bridge spanning-tree errdisable-timeout

Use this command to enable the error-disable-timeout facility, which sets a timeout for ports that are disabled due to the BPDU guard feature.

The BPDU guard feature shuts down the port on receiving a BPDU on a BPDU-guard enabled port. This command associates a timer with the feature such that the port gets enabled back without manual intervention after a set interval.

Use the `no` parameter to disable the error-disable-timeout facility.

Command Syntax

```
bridge <1-32> spanning-tree errdisable-timeout enable
no bridge <1-32> spanning-tree errdisable-timeout enable
```

Parameters

`<1-32>`	Specify the bridge group ID.
`enable`	Enable the timeout mechanism for the port to be enabled back

Default

By default, the port is enabled after 300 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 spanning-tree errdisable-timeout enable
```

bridge spanning-tree force-version

Use this command to set the version for the bridge. A version identifier of less than a value of 2 enforces the spanning tree protocol. Although the command supports an input range of 0-4, for RSTP, the valid range is 0-2. When the force-version is set for a bridge, all ports of the bridge have the same spanning tree version set.

Use the `show spanning tree` command to display administratively configured and currently running values of the BPDU filter parameter for the bridge and port (see show spanning-tree).

Use the no parameter with this command to disable the version for the bridge.

Command Syntax

```
bridge <1-32> spanning-tree force-version <0-4>
no bridge <1-32> spanning-tree force-version
```

Parameters

`<1-32>`	Specify the bridge group ID.
`force-version`	Specify a force version identifier:
`0`	STP
`1`	Not supported
`2`	RSTP
`3`	MSTP

Default

By default, spanning tree force version is 0

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

Set the value to enforce the spanning tree protocol:

```
#configure terminal
(config)#bridge 1 spanning-tree force-version 0

(config)#no bridge 1 spanning-tree force-version
```

bridge spanning-tree pathcost

Use this command to set a spanning-tree path cost method.

If the short parameter is used, the switch uses a value for the default path cost a number in the range 1 through 65,535. If the long parameter is used, the switch uses a value for the default path cost a number in the range 1 through 200,000,000. Use the show spanning-tree to view the administratively configured and current running pathcost method running on a bridge.

Use the `no` option with this command to return the path cost method to the default setting.

Command Syntax

```
bridge <1-32> spanning-tree pathcost method (short|long)
no bridge <1-32> spanning-tree pathcost method
```

Parameters

`<1-32>`	Specify the bridge group ID.
`method`	Method used to calculate default port path cost.
`long`	Use 16-bit based values for default port path costs.
`short`	Use 32-bit based values for default port path costs.

Default

By default, path cost method for STP is short and for MSTP/RSTP is long.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 spanning-tree pathcost method short

(config)#no bridge 1 spanning-tree pathcost method
```

bridge spanning-tree portfast

Use this command to set the portfast BPDU (Bridge Protocol Data Unit) guard or filter for the bridge.

Use the `show spanning tree` command to display administratively configured and currently running values of the BPDU filter parameter for the bridge and port (see show spanning-tree).

Use the `no` parameter with this command to disable the BPDU filter for the bridge.

BPDU Filter

All ports that have their BPDU filter set to default take the same value of BPDU filter as that of the bridge. The Spanning Tree Protocol sends BPDUs from all ports. Enabling the BPDU Filter feature ensures that PortFast-enabled ports do not transmit or receive any BPDUs.

Note: On BPDU-Filter enabled port when BPDU is received the interface loses its port-fast operational status and re-enable the spanning-tree operation. Hence the "spanning-tree portfast" is removed from the interface which is an expected behavior.

BPDU Guard

When the BPDU guard feature is set for a bridge, all portfast-enabled ports of the bridge that have the BPDU guard set to default shut down the port on receiving a BPDU. In this case, the BPDU is not processed. You can either bring the port back up manually by using the `no shutdown` command, or configure the errdisable-timeout feature to enable the port after the specified time interval.

Command Syntax

```
bridge <1-32> spanning-tree portfast bpdu-guard
bridge <1-32> spanning-tree portfast bpdu-filter
no bridge <1-32> spanning-tree portfast bpdu-guard
no bridge <1-32> spanning-tree portfast bpdu-filter
```

Parameters

`<1-32>`	Specify the bridge group ID.
`bpdu-filter`	Specify to filter the BPDUs on portfast enabled ports.
`bpdu-guard`	Specify to guard the portfast ports against BPDU receive.

Default

By default, portfast for STP is enabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#bridge 3 spanning-tree portfast bpdu-filter
```

```
#configure terminal
(config)#bridge 1 spanning-tree portfast bpdu-guard
```

bridge te-msti

Use this command to enable or disable a Multiple Spanning Tree Instance (MSTI).

The te-msti always refers to the MST instance indexed by the pre-defined macro constant MSTP_TE_MSTID internally. This is the only MST instance which supports the disabling of spanning trees.

Use the no form of this command to remove the configuration.

Command Syntax

```
bridge (<1-32> | backbone) te-msti
no bridge (<1-32> | backbone) te-msti
```

Parameters

<1-32>	Specify the bridge group ID.
backbone	Identity of the backbone bridge group.
te-msti	MSTI to be the traffic engineering MSTI instance.

Default

By default, bridge te-msti is disabled

Command Mode

TE-MSTI Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree te-msti configuration
(config-te-msti)#bridge 2 te-msti

(config-te-msti)#no bridge 2 te-msti
```

bridge te-msti vlan

Use this command to enable or disable a Multiple Spanning Tree Instance (MSTI). When an MSTI is shutdown (disabled) each VLAN in the MSTI is set to the forwarding state on all bridge ports which the VLAN as a member of. When and MSTI is enabled (no shutdown), normal MSTP operation is started for the MSTI.

The te-msti always refers to the MST instance indexed by the pre-defined macro constant MSTP_TE_MSTID internally. This is the only MST instance which supports the disabling of spanning trees. All VLANs that do not want spanning tree topology computation need to be assigned to this te-msti instance.

This command is intended for supporting Traffic Engineering (TE) Ethernet tunnels. All VLANs allocated for traffic engineering should be assigned to one MSTI. That MSTI can in turn shutdown the spanning tree operation so that each VLAN path through the network can be manually provisioned.

Use the no form of this command to remove the configuration.

Command Syntax

```
bridge (<1-32> | backbone) te-msti vlan <1-4094>
no bridge (<1-32> | backbone) te-msti vlan <1-4094>
```

Parameters

<1-32>	Specify the bridge group ID.
backbone	Identity of the backbone bridge group.
vlan	Specify a VLAN.
<1-4094>	Specify a VLAN identifier to be associated.

Note: This designated instance is defined in 802.1Qay clause 8.9 to be 0xFFE.

Default

By default, te-msti vlan is vlan1.

Command Mode

TE-MSTI Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree te-msti configuration
(config-te-msti)#bridge 2 te-msti vlan 10
(config-te-msti)#no bridge 2 te-msti vlan 10
```

bridge-group instance

Use this command to assign a Multiple Spanning Tree (MST) instance to a port.

Use the `no` form of this command to remove the interface from the MST instance.

Command Syntax

```
bridge-group (<1-32> | backbone) instance (<1-63> | te-msti)
no bridge-group (<1-32> | backbone) instance (<1-63> | te-msti)
```

Parameters

`<1-32>`	Bridge identifier.
`backbone`	Backbone bridge.
`<1-63>`	Multiple spanning tree instance identifier.
`te-msti`	Traffic engineering MSTI instance.
	For Provider Backbone Bridging (PBB), bridge-group <1-32> refers to the I-component or PB bridge while the <backbone> bridge group refers to the B-component. Usually for a BEB (Backbone Edge Bridge) device, the backbone bridge-group is used for traffic engineering.
	For a PB (Provider Bridge) device used as BCB (Backbone Core Bridge), bridge group <1-32> is used for traffic engineering.

Default

By default, the bridge port remains in the listening and learning states for 15 seconds before transitional to the forwarding state.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#bridge-group 1
(config-if)#bridge-group 1 instance te-msti
```

bridge-group instance path-cost

Use this command to set a path cost for a multiple spanning tree instance.

Before you can give this command, you must explicitly add an MST instance to a port using the `bridge-group instance` command.

Use the `no` form of this command to set the path cost to its default which varies depending on bandwidth.

Command Syntax

```
bridge-group (<1-32> | backbone) instance <1-63> path-cost <1-200000000>
no bridge-group ( <1-32> | backbone) instance <1-63> path-cost
```

Parameters

`<1-32>`	Bridge identifier.
`backbone`	Specify the backbone bridge.
`<1-63>`	Set the MST instance identifier.
`<1-200000000>`	Path cost for a port (a lower path cost means greater likelihood of becoming root).

Default

Assuming a 10 Mb/s link speed, the default value is 200,000.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#bridge 4 instance 3 vlan 3
(config-mst)#exit
(config)#interface eth1
(config-if)#bridge-group 4 instance 3
(config-if)#bridge-group 4 instance 3 path-cost 1000
```

bridge-group instance priority

Use this command to set the priority of a multiple spanning tree instance.

The Multiple Spanning Tree Protocol uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies a better priority. In the case of the same priority, the interface index will serve as the tiebreaker, with the lower-numbered interface being preferred over others.

Command Syntax

```
bridge-group (<1-32>) instance (<1-63>) priority <0-240>
no bridge-group (<1-32>) instance (<1-63>) priority
```

Parameters

`<1-32>`	Bridge identifier.
`backbone`	Backbone bridge.
`<1-63>`	Multiple spanning tree instance identifier.
`<0-240>`	Port priority. A lower value means greater likelihood of becoming root. Set the port priority in increments of 16.

Default

By default, the port priority is 128

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface eth2
(config-if)#bridge-group 2
(config-if)#bridge-group 2 instance 4
(config-if)#bridge-group 2 instance 4 priority 64
```

bridge-group path-cost

Use this command to set the cost of a path. Before you can use this command to set a path-cost in a VLAN configuration, you must explicitly add an MST instance to a port using the `bridge-group instance` command.

Use the `no` parameter with this command to restore the default cost value of the path which varies depending on the bandwidth.

Command Syntax

```
bridge-group <1-32> path-cost <1-200000000>
no bridge-group <1-32> path-cost
```

Parameters

`<1-32>`	Specify the bridge group ID.
`path-cost`	Specify the cost of path for a port.
`<1-200000000>`	Specify the cost of the path (a lower cost means a greater likelihood of the interface becoming root).

Default

Assuming a 10 Mb/s link speed, the default value is 200,000.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#bridge 4 instance 3 vlan 3
(config-mst)#exit
(config)#interface eth1
(config-if)#bridge-group 4
(config-if)#bridge-group 4 path-cost 1000
```

bridge-group priority

Use this command to set the port priority for a bridge group.

The Multiple Spanning Tree Protocol uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies a better priority. In the case of the same priority, the interface index will serve as the tiebreaker, with the lower-numbered interface being preferred over others.

Command Syntax

```
bridge-group (<1-32> | backbone) priority <0-240>
no bridge-group (<1-32> | backbone) priority
```

Parameters

`<1-32>`	Specify the bridge group ID.
`backbone`	Backbone bridge.
`<0-240>`	Specify the port priority (a lower priority indicates greater likelihood of the interface becoming a root). The priority values can only be set in increments of 16.

Default

By default, port priority for each instance is 128

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#bridge-group 4 priority 80
```

bridge-group spanning-tree

This command is used to enable or disable the spanning-tree on a configured bridge.

Command Syntax

```
bridge-group <1-32> spanning-tree (disable|enable)
```

Parameters

`<1-32>`	Specify the bridge group ID.
`disable`	Disable spanning tree on the interface.
`enable`	Enable spanning tree on the interface.

Default

By default, spanning-tree is enabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface eth1
(config-if)#bridge-group 1 spanning-tree enable
```

clear spanning-tree detected protocols

Use this command to clear the detected protocols for a specific bridge or interface. This command begins the port migration as per IEEE 802.1w-2001, Section 17.26. After issuing this command, the migration timer is started on the port, only if the force version is RSTP or MSTP (greater versions of RSTP).

Command Syntax

```
clear spanning-tree detected protocols bridge <1-32>
```

Parameters

`<1-32>`	Specify the bridge group ID.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear spanning-tree detected protocols bridge 2
```

clear spanning-tree statistics

Use this command to clear all STP BPDU statistics.

Command Syntax

```
clear spanning-tree statistics bridge <1-32>
clear spanning-tree statistics interface IFNAME (instance (<1-63>)| vlan <1-4094>)
  bridge <1-32>
clear spanning-tree statistics (interface IFNAME| (instance (<1-63>)| vlan <2-
  4094>)) bridge <1-32>
```

Parameters

<1-32>	Specify the bridge identifier.
IFNAME	Specify the name of the interface on which protocols have to be cleared.
<1-63>	MST instance ID.
<1-4094>	VLAN identifier where spanning tree is located <2-4094>

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear spanning-tree statistics bridge 32
```

customer-spanning-tree customer-edge path-cost

Use this command to set the cost of a path associated with a customer edge port on a customer edge spanning tree.

Use the `no` form of this command to remove the cost of a path associated with a customer edge port on a customer edge spanning tree.

Command Syntax

```
customer-spanning-tree customer-edge path-cost <1-200000000>
no customer-spanning-tree customer-edge path-cost
```

Parameters

`path-cost`	Specify the path-cost of a port.
`<1-200000000>`	Specify the cost to be assigned to the group.

Default

Assuming a 10 Mb/s link speed, the default value is 200,000

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree customer-edge path-cost 1000
```

customer-spanning-tree customer-edge priority

Use this command to set the port priority for a customer-edge port in the customer spanning tree.

Command Syntax

```
customer-spanning-tree customer-edge priority <0-240>
```

Parameters

`priority`	Specify the port priority.
`<0-240>`	Specify the port priority range (a lower priority indicates greater likelihood of the interface becoming a root). The priority values can only be set in increments of 16.

Default

By default, priority is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree customer-edge priority 100
```

customer-spanning-tree forward-time

Use this command to set the time (in seconds) after which (if this bridge is the root bridge) each port changes states to learning and forwarding. This value is used by all instances.

Use the `no` form of this command to restore the default value of 15 seconds.

Command Syntax

```
customer-spanning-tree forward-time <4-30>
no customer-spanning-tree forward-time
```

Parameters

`<4-30>`	Specify the forwarding time delay in seconds.

Note: Care should be exercised if the value is set to less than 7 seconds.

Default

By default, priority is 15 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree forward-time 6

(config-if)#no customer-spanning-tree forward-time
```

customer-spanning-tree hello-time

Use this command to set the hello-time, the time in seconds after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange Bridge Protocol Data Units (BPDUs). Avoid a very low value of this parameter as this can lead to excessive traffic on the network; a higher value delays the detection of topology change. This value is used by all instances.

Use the `no` option with this command to restore the default value of the hello-time.

Command Syntax

```
customer-spanning-tree hello-time <1-10>
no customer-spanning-tree hello-time
```

Parameters

`<1-10>`	Specify the hello BPDU interval in seconds.

Default

By default, level is 2 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree hello-time 3

(config-if)#no customer-spanning-tree hello-time
```

customer-spanning-tree max-age

Use this command to set the max-age for a bridge.

Max-age is the maximum time in seconds for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. The value of max-age should be greater than twice the value of hello-time plus one, but less than twice the value of forward delay minus one. The allowable range for max-age is 6-40 seconds. Configure this value sufficiently high, so that a frame generated by a root can be propagated to the leaf nodes without exceeding the max-age.

Use the `no` parameter with this command to restore the default value of max-age.

Command Syntax

```
customer-spanning-tree max-age <6-40>
no customer-spanning-tree max-age
```

Parameters

`<6-40>`	Specify the maximum time in seconds to listen for the root bridge.

Default

By default, bridge max-age is 20 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree max-age 12

(config-if)#no customer-spanning-tree max-age
```

customer-spanning-tree priority

Use this command to set the bridge priority for the spanning tree on a customer edge port. Using a lower priority indicates a greater likelihood of the bridge becoming root. This command must be used to set the priority of the customer spanning tree running on the customer edge port.

Use the `no` form of the command to reset it to the default value.

Command Syntax

```
customer-spanning-tree priority <0-61440>
no customer-spanning-tree priority
```

Parameters

`<0-61440>`	Specify the bridge priority in the range <0-61440>. Priority values can be set only in increments of 4096.

Default

By default, priority is 61440

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree priority 4096

(config-if)#no customer-spanning-tree priority
```

customer-spanning-tree provider-edge path-cost

Use this command to set the cost of a path associated with a provider edge port on a customer edge spanning tree.

Use the `no` form of this command to remove the cost of a path associated with a provider edge port on a customer edge spanning tree.

Command Syntax

```
customer-spanning-tree provider-edge svlan <1-4094> path-cost <1-200000000>
no customer-spanning-tree provider-edge svlan <1-4094> path-cost
```

Parameters

`<1-4094>`	Specify the SVLAN identifier of provider edge port.
`<1-200000000>`	Specify the cost to be assigned to the group.

Default

Assuming a 10 Mb/s link speed, the default value is 200,000

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree provider-edge svlan 2 path-cost 1000

(config-if)#no customer-spanning-tree provider-edge svlan 2 path-cost
```

customer-spanning-tree provider-edge priority

Use this command to set the port priority for a provider-edge port in the customer spanning tree.

Command Syntax

```
customer-spanning-tree provider-edge svlan <1-4094> priority <0-240>
```

Parameters

`<1-4094>`	Specify the SVLAN identifier of provider edge port.
`<0-240>`	Specify the port priority (a lower priority means greater likelihood of the interface becoming root). The priority values can only be set in increments of 16.

Default

By default, priority is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree provider-edge svlan 2 priority 0
```

customer-spanning-tree transmit-holdcount

Use this command to set the transmit-holdcount for a bridge.

Use the `no` parameter with this command to restore the default value of `transmit-holdcount`.

Command Syntax

```
customer-spanning-tree transmit-holdcount <1-10>
no customer-spanning-tree transmit-holdcount
```

Parameters

`<1-10>`	Specify the maximum number that can be transmitted per second.

Default

By default, bridge transmit hold count is 6

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree transmit-holdcount 3

(config-if)#no customer-spanning-tree transmit-holdcount
```

debug mstp

Use this command to turn on, and turn off, debugging and echoing data to the console, at various levels.

Note: This command enables MSTP, RSTP, and STP debugging.

Use the `no` parameter with this command to turn off debugging.

Command Syntax

```
debug mstp all
debug mstp cli
debug mstp packet rx
debug mstp packet tx
debug mstp protocol
debug mstp protocol detail
debug mstp timer
debug mstp timer detail
no debug mstp all
no debug mstp cli
no debug mstp packet rx
no debug mstp packet tx
no debug mstp protocol
no debug mstp protocol detail
no debug mstp timer
no debug mstp timer detail
```

Parameters

`all`	Echoes all spanning-tree debugging levels to the console.
`cli`	Echoes spanning-tree commands to the console.
`packet`	Echoes spanning-tree packets to the console.
`rx`	Received packets.
`tx`	Transmitted packets.
`protocol`	Echoes protocol changes to the console.
`detail`	Detailed output.
`timer`	Echoes timer start to the console.
`detail`	Detailed output.

Command Mode

Exec, Privileged Exec, and Configure modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug mstp all
(config)#debug mstp cli
(config)#debug mstp packet rx
(config)#debug mstp protocol detail
(config)#debug mstp timer
```

show debugging mstp

Use this command to display the status of debugging of the MSTP system.

Command Syntax

```
show debugging mstp
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debugging mstp
MSTP debugging status:
MSTP debugging status:
 MSTP timer debugging is on
 MSTP protocol debugging is on
 MSTP detailed protocol debugging is on
 MSTP cli echo debugging is on
 MSTP transmitting packet debugging is on
 MSTP receiving packet debugging is on
#
```

show spanning-tree

Use this command to show the state of the spanning tree for all STP or RSTP bridge-groups, including named interface and VLANs.

Command Syntax

```
show spanning-tree
show spanning-tree interface IFNAME
show spanning-tree mst
show spanning-tree mst config
show spanning-tree mst interface IFNAME
show spanning-tree mst detail
show spanning-tree mst detail interface IFNAME
show spanning-tree mst instance (<1-63>) interface IFNAME
show spanning-tree mst instance (<1-63> | te-msti)
show spanning-tree statistics bridge <1-32>
show spanning-tree statistics interface IFNAME (instance (<1-63>)| vlan <2-4094>)
  bridge <1-32>
show spanning-tree statistics (interface IFNAME | (instance (<1-63>) | vlan <1-
  4094>)) bridge <1-32>
show spanning-tree vlan range-index
```

Parameters

`interface`	Display interface information
`mst`	Display MST information
`statistics`	Display statistics of the BPDUs
`vlan range-index`	Display a VLAN range-index value
`config`	Display configuration information
`detail`	Display detailed information
`instance`	Display instance information
`<1-63>`	Specify the instance identifier
`te-msti`	Display Traffic Engineering MSTI instance
`<1-32>`	Specify the bridge identifier
`IFNAME`	Display the interface name
`<2-4094>`	Specify a VLAN identifier, associated with the instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of this command displaying spanning tree information.

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000002b328530a
% 1: Bridge Id 80000002b328530a
% 1: last topology change Wed Nov 19 22:39:18 2008
% 1: 11 topology change(s) - last topology change Wed Nov 19 22:39:18 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%eth2: Ifindex 5 - Port Id 8005 - Role Designated - State Forwarding
%eth2: Designated Path Cost 0
%eth2: Configured Path Cost 200000 - Add type Explicit ref count 1
%eth2: Designated Port Id 8005 - Priority 128 -
%eth2: Root 80000002b328530a
%eth2: Designated Bridge 80000002b328530a
%eth2: Message Age 0 - Max Age 20
%eth2: Hello Time 2 - Forward Delay 15
%eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%eth2: forward-transitions 4
%eth2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%eth2: No portfast configured - Current portfast off
%eth2: portfast bpdu-guard default - Current portfast bpdu-guard off
%eth2: portfast bpdu-filter default - Current portfast bpdu-filter off
%eth2: no root guard configured- Current root guard off
%eth2: Configured Link Type point-to-point - Current point-to-point
%eth1: Ifindex 4 - Port Id 8004 - Role Designated - State Forwarding
%eth1: Designated Path Cost 0
%eth1: Configured Path Cost 200000 - Add type Explicit ref count 1
%eth1: Designated Port Id 8004 - Priority 128 -
%eth1: Root 80000002b328530a
%eth1: Designated Bridge 80000002b328530a
%eth1: Message Age 0 - Max Age 20
%eth1: Hello Time 2 - Forward Delay 15
%eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%eth1: forward-transitions 4
%eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%eth1: No portfast configured - Current portfast off
%eth1: portfast bpdu-guard default - Current portfast bpdu-guard off
%eth1: portfast bpdu-filter default - Current portfast bpdu-filter off
%eth1: no root guard configured- Current root guard off
%eth1: Configured Link Type point-to-point - Current point-to-point
%
%
```

The following is a sample output of this command displaying the state of the spanning tree for interface eth1.

```
#show spanning-tree interface eth1
```

```
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000002b328530a
% 1: Bridge Id 80000002b328530a
% 1: last topology change Wed Nov 19 22:39:18 2008
% 1: 11 topology change(s) - last topology change Wed Nov 19 22:39:18 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% eth1: Ifindex 4 - Port Id 8004 - Role Designated - State Forwarding
% eth1: Designated Path Cost 0
% eth1: Configured Path Cost 200000 - Add type Explicit ref count 1
% eth1: Designated Port Id 8004 - Priority 128 -
% eth1: Root 80000002b328530a
% eth1: Designated Bridge 80000002b328530a
% eth1: Message Age 0 - Max Age 20
% eth1: Hello Time 2 - Forward Delay 15
% eth1: forward-transitions 4
% eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
% eth1: No portfast configured - Current portfast off
% eth1: portfast bpdu-guard default - Current portfast bpdu-guard off
% eth1: portfast bpdu-filter default - Current portfast bpdu-filter off
% eth1: no root guard configured- Current root guard off
```

Table 4-14 Explains the show command output fields.

Table 4-14: show spanning-tree interface output fields

Field	Description
Bridge up	A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments.
Root Path Cost	Root cost for the interface.
Root Port	Interface that is the current elected root port for this bridge.
Bridge Priority	Used for the common instance.
Forward Delay	Configured time an STP bridge port remains in the listening and learning states before transitioning to the forwarding state.
Hello Time	Configured number of seconds between transmissions of configuration BPDUs.
Max Age	Maximum age of received protocol BPDUs.
Port Id	Logical interface identifier configured to participate in the MSTP instance.
Role Designated	Designated role for the packets in the interface.
State Forwarding	State of the forwarding packets in the interface.
Designated Path Cost	Designated cost for the interface.

Field	Description
Configured Path Cost	Configured cost for the interface.
Designated Port Id	Port ID of the designated port for the LAN segment this interface is attached to.
Priority	Specify the port priority.
Message Age	Number of seconds elapsed since the most recent BPDU was received.
Forward Timer	The forward delay timer is the time interval that is spent in the listening and learning state.
Msg Age Timer	The message age contains the length of time that has passed since the root bridge initially originated the BPDU.
Received RSTP	Number of times the received the RSTP.
Send RSTP	Number of times transmitted the RSTP.

show spanning-tree mst

Use this command to display the filtering database values. This command displays the number of instances created, and VLANs associated with it.

Command Syntax

```
show spanning-tree mst
show spanning-tree mst config
show spanning-tree mst detail
show spanning-tree mst detail interface IFNAME
show spanning-tree mst instance (<1-63>) interface IFNAME
show spanning-tree mst instance (<1-63> | te-msti)
show spanning-tree mst interface IFNAME
```

Parameters

`config`	Display configuration information.
`detail`	Display detailed information.
`interface`	Display interface information.
`instance`	Display instance information.
`<1-63>`	Specify the instance identifier.
`te-msti`	Traffic Engineering MSTI instance.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show spanning-tree mst
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge
Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000002b328530a
% 1: CIST Reg Root Id 80000002b328530a
% 1: CIST Bridge Id 80000002b328530a
% 1: 2 topology change(s) - last topology change Wed Nov 19 22:43:21 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec%
% Instance VLAN
% 0:        1
% 2:        3-4
```

Table 4-15 Explains the show command output fields.

Table 4-15: show spanning-tree mst output fields

Field	Description
Bridge up	A network bridge is networking process that creates a single aggregate network from multiple communication networks or network segments.
CIST Root Path Cost	Calculated cost to reach the regional root bridge from the bridge where the command is entered.
CIST Root Port	Interface that is the current elected CIST root port for this bridge.
CIST Bridge	A CIST bridge is networking process that creates a single aggregate network from multiple communication networks.
Priority	Specify the port priority.
Forward Delay	Configured time an STP bridge port remains in the listening and learning states before transitioning to the forwarding state.
Hello Time	Configured number of seconds between transmissions of configuration BPDUs.
Max Age	Maximum age of received protocol BPDUs.
Max-hops	Configured maximum number of hops a BPDU can be forwarded in the MSTP region.

show spanning-tree statistics

Use this command to display detailed BPDU statistics for a spanning tree instance.

Command Syntax

```
show spanning-tree statistics bridge <1-32>
show spanning-tree statistics interface IFNAME (instance (<1-63>)| vlan <2-4094>)
  bridge <1-32>
show spanning-tree statistics (interface IFNAME | (instance (<1-63>) | vlan <1-
  4094>)) bridge <1-32>
```

Parameters

`<1-32>`	Bridge identifier.
`<1-63>`	MST instance identifier.
`IFNAME`	Displays the interface name.
`<2-4094>`	Specify a VLAN identifier, associated with the instance.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In the following example, bridge-group 1 is configured for IEEE on the eth2 interface.

```
#show spanning-tree statistics interface eth2 bridge 1

                Port number = 4 Interface = eth2
                ================================
% BPDU Related Parameters
% ----------------------
% Port Spanning Tree                : Enable
% Spanning Tree Type                : Spanning Tree Protocol
% Current Port State                : Forwarding
% Port ID                           : 8004
% Port Number                       : 4
% Path Cost                         : 19
% Message Age                       : 0
% Designated Root                   : 80:00:52:54:00:b2:49:c1
% Designated Cost                   : 0
% Designated Bridge                 : 80:00:52:54:00:b2:49:c1
% Designated Port Id                : 0x8004
% Top Change Ack                    : FALSE
% Config Pending                    : FALSE

% PORT Based Information & Statistics
```

```
% ------------------------------------
% Config Bpdu's xmitted              : 54327
% Config Bpdu's received             : 0
% TCN Bpdu's xmitted                 : 50
% TCN Bpdu's received                : 3
% Forward Trans Count                : 1

% STATUS of Port Timers
% ---------------------
% Hello Time Configured              : 2
% Hello timer                        : ACTIVE
% Hello Time Value                   : 0
% Forward Delay Timer                : INACTIVE
% Forward Delay Timer Value          : 0
% Message Age Timer                  : INACTIVE
% Message Age Timer Value            : 0
% Topology Change Timer              : INACTIVE
% Topology Change Timer Value        : 0
% Hold Timer                         : INACTIVE
% Hold Timer Value                   : 0

% Other Port-Specific Info
  ------------------------
% Max Age Transitions                : 1
% Msg Age Expiry                     : 0
% Similar BPDUS Rcvd                 : 0
% Src Mac Count                      : 0
% Total Src Mac Rcvd                 : 3
% Next State                         : Discard/Blocking
% Topology Change Time               : 0


% Other Bridge information & Statistics
  -------------------------------------
% STP Multicast Address              : 01:80:c2:00:00:00
% Bridge Priority                    : 32768
% Bridge Mac Address                 : 80:00:52:54:00:b2
% Bridge Hello Time                  : 2
% Bridge Forward Delay               : 15
% Topology Change Initiator          : 5
% Last Topology Change Occured       : Wed Feb 17 09:39:58 2021
% Topology Change                    : FALSE
% Topology Change Detected           : FALSE
% Topology Change Count              : 5
% Topology Change Last Recvd from    : 00:00:00:00:00:00
```

Table 4-16 Explains the show command output fields.

Table 4-16: show spanning-tree statistics output fields

Field	Description
BPDU Related Parameters	Details of the BPDU related parameters.
PORT Based Information & Statistics	Information of the port and interface for which the statistics are being displayed.
STATUS of Port Timers	Status of the port timers.
Other Port-Specific Info	Specific information about the port.
Other Bridge information & Statistics	Information about bridge and statistics being displayed.

spanning-tree autoedge

Use this command to assist in automatic identification of the edge port.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
spanning-tree autoedge
no spanning-tree autoedge
```

Default

By default, spanning-tree autoedge is disabled

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree autoedge
```

spanning-tree edgeport

Use this command to set a port as an edge-port and to enable rapid transitions.

Use the `no` parameter with this command to set a port to its default state (not an edge-port) and to disable rapid transitions.

Note: This command is an alias to the `spanning-tree portfast` command. Both commands can be used interchangeably.

Command Syntax

```
spanning-tree edgeport
no spanning-tree edgeport
```

Default

By default, spanning-tree edgeport is disabled

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree edgeport
```

spanning-tree guard

Use this command to enable the root guard feature for the port. This feature disables reception of superior BPDUs.

The root guard feature makes sure that the port on which it is enabled is a designated port. If the root guard enabled port receives a superior BPDU, it goes to a Listening state (for STP) or discarding state (for RSTP and MSTP).

Use the `no` parameter with this command to disable the root guard feature for the port.

Command Syntax

```
spanning-tree guard root
no spanning-tree guard root
```

Parameters

`root`	Set to disable reception of superior BPDUs

Default

By default, spanning-tree guard root is enabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree guard root
```

spanning-tree instance restricted-role

Use this command to set the restricted role value for the instance to TRUE.

Use the `no` parameter with this command to set the restricted role value for the instance to FALSE.

Command Syntax

```
spanning-tree instance <1-63> restricted-role
no spanning-tree instance <1-63> restricted-role
```

Parameters

`<1-63>`	Specify the instance ID range.

Default

By default, restricted-role value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree instance 2 restricted-role
```

spanning-tree instance restricted-tcn

Use this command to set the restricted TCN value for the instance to TRUE.

Command Syntax

```
spanning-tree instance <1-63> restricted-tcn
no spanning-tree instance <1-63> restricted
```

Parameters

<1-63>	Specify the instance ID range.

Default

By default, restricted TCN value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree instance 2 restricted-tcn
```

spanning-tree link-type

Use this command to enable or disable point-to-point or shared link types.

RSTP has a backward-compatible STP mode, `spanning-tree link-type shared`. An alternative is the `spanning-tree force-version 0`.

Use the `no` parameter with this command to disable rapid transition.

Command Syntax

```
spanning-tree link-type auto
spanning-tree link-type point-to-point
spanning-tree link-type shared
no spanning-tree link-type
```

Parameters

`auto`	Sets to either point-to-point or shared based on duplex state.
`point-to-point`	Enables rapid transition.
`shared`	Disables rapid transition.

Default

By default, spanning-tree link-type is enabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree link-type point-to-point

(config-if)#no spanning-tree link-type
```

spanning-tree mst configuration

Use this command to enter the Multiple Spanning Tree Configuration mode.

Command Syntax

```
spanning-tree mst configuration
```

Parameters

None

Default

No default value is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#
```

spanning-tree bpdu-filter

Use this command to set the BPDU filter value for individual ports. When the `enable` or `disable` parameter is used with this command, this configuration takes precedence over bridge configuration. However, when the `default` parameter is used with this command, the bridge level BPDU filter configuration takes effect for the port.

Use the `show spanning tree` command to display administratively configured and currently running values of the BPDU filter parameter for the bridge and port (see show spanning-tree).

Use the `no` parameter with this command to revert the port BPDU filter value to default.

Command Syntax

```
spanning-tree bpdu-filter (enable|disable|default)
no spanning-tree bpdu-filter
```

Parameters

`default`	Sets the bpdu-filter to the default level.
`disable`	Disables the BPDU-filter.
`enable`	Enables the BPDU-filter.

Default

By default, spanning-tree bpdu-filter is default option

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree bpdu-filter enable

(config-if)#no spanning-tree bpdu-filter
```

spanning-tree bpdu-guard

Use this command to enable or disable the BPDU Guard feature on a port.

This command supersedes the bridge level configuration for the BPDU Guard feature. When the `enable` or `disable` parameter is used with this command, this configuration takes precedence over bridge configuration. However, when the `default` parameter is used with this command, the bridge-level BPDU Guard configuration takes effect.

Use the `show spanning tree` command to display administratively configured and currently running values of the BPDU filter parameter for the bridge and port (see show spanning-tree).

Use the no parameter with this command to set the BPDU Guard feature on a port to default.

Command Syntax

```
spanning-tree bpdu-guard (enable|disable|default)
no spanning-tree bpdu-guard
```

Parameters

`default`	Sets the BPDU-guard to the default level.
`disable`	Disables the BPDU-guard.
`enable`	Enables the BPDU-guard.

Default

By default, spanning-tree bpdu-guard is default

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree bpdu-guard enable

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

spanning-tree restricted-domain-role

Use this command to set the restricted-domain-role value of the port to TRUE.

Use the `no` parameter with this command to set the restricted-domain-role value of the port to FALSE.

Command Syntax

```
spanning-tree restricted-domain-role
no spanning-tree restricted-domain-role
```

Parameters

None

Default

By default, restricted-role value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree restricted-domain-role
```

spanning-tree restricted-role

Use this command to set the restricted-role value of the port to TRUE.

Use the `no` parameter with this command to set the restricted-role value of the port to FALSE.

Command Syntax

```
spanning-tree restricted-role
no spanning-tree restricted-role
```

Parameters

None

Default

By default, restricted-role value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree restricted-role
```

spanning-tree restricted-tcn

Use this command to set the restricted TCN value of the port to TRUE.

Use the `no` parameter with this command to set the restricted TCN value of the port to FALSE.

Command Syntax

```
spanning-tree restricted-tcn
no spanning-tree restricted-tcn
```

Parameters

None

Default

By default, restricted TCN value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree restricted-tcn
```

spanning-tree te-msti configuration

This command is used to put the terminal into the `te-msti` configuration mode.

After creating a bridge instance and adding VLAN to that bridge instance, use this command to enter `te-msti` configuration mode.

Command Syntax

```
spanning-tree te-msti configuration
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree te-msti configuration
(config-te-msti)#
```

CHAPTER 5 Link Aggregation Commands

This chapter describes link aggregation commands.

channel-group mode

Use this command to add an interface to an existing link aggregation group.

After you execute this command, the interface loses its properties and takes the properties of the aggregated interface.

Use the `no` parameter with this command to remove an interface from a dynamic link aggregation group. When you remove an interface from a LAG, the interface acquires the default interface properties.

Command Syntax

```
channel-group <1-16383> mode (active|passive)
no channel-group
```

Parameters

`<1-16383>`	Specify a channel group number (with DRNI).
`mode`	Specify a channel mode.
`active`	Enable LACP negotiation.
`passive`	Disable LACP negotiation.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#channel-group 1 mode active
(config-if)#exit

#sh run in po1
!
interface po1
 switchport
```

The is an example of `no channel-group`:

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#no channel-group
(config-if)#exit

#sh run in xe1
!
interface xe1 switchport
!
#sh run in po1
!
```

```
interface po1
 switchport

!
```

clear lacp

Use this command to clear the counters of all LACP aggregators or a given LACP aggregator.

Command Syntax

```
clear lacp <1-16383> counters
clear lacp counters
```

Parameters

`<1-16383>`	Clears a channel-group number.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear lacp 2 counters
```

debug lacp

Use this command to enable LACP debugging.

Use the `no` parameter with this command to disable debugging.

Command Syntax

```
debug lacp (event|cli|timer|packet|sync|ha|all|rx|tx)
no debug lacp (event|cli|timer|packet|sync|ha|allrx|tx)
```

Parameters

`all`	Enables all LACP debugging.
`cli`	Echo commands to console.
`event`	Sets the debug options for LACP events.
`ha`	Echo High availability events to console.
`packet`	Sets the debug option for LACP packets.
`sync`	Echo synchronization to console.
`timer`	Echo timer expiry to console.
`rx`	Echo receiving of lacpdus to console.
`tx`	Echo transmission of lacpdus to console.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug lacp all
```

interface po

Use this command to create a dummy dynamic link aggregate interface (by default an L3 LAG interface).

Use the `no` form of this command to remove a dynamic link aggregate group and also it remove the properties of the po from all member ports.

Note: Switchport/routed mode needs to be set for the PO before adding member ports to it.

Command Syntax

```
interface po<1-16383>
no interface po<1-16383>
```

Parameters

`<1-16383>`	Channel group number.

Default

By default, interface po is L3 LAG interface

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface po1
(config-if)#switchport
(config-if)#exit
```

interface sa

Use this command to create a dummy static link aggregate interface (by default an L3 LAG interface) and to add an interface to an existing static link aggregation group.

Use the `no` form of this command to remove a static link aggregate group and also remove the properties of the po from all member ports.

Command Syntax

```
interface sa<1-16383>
no interface sa<1-16383>
```

Parameters

`<1-16383>`	Channel group number.

Default

By default, interface sa is L3 LAG interface

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface sa1
(config-if)#switchport
(config-if)#exit
```

lacp destination-mac

Use this command to set the address type to use for sending LACPDUs (Link Aggregation Control Protocol Data Units).

Note: The interface must be an aggregation port.

Use the `no` form of this command to set the address type to its default (multicast group address).

Command Syntax

```
lacp destination-mac  (customer-bridge-group-address | multicast-group-address |
  non-tmpr-group-address)
no lacp destination-mac
```

Parameters

`customer-bridge-group-address`

Customer bridge group address

`multicast-group-address`

Multicast group address (default)

`non-TPMR-group-address`

Non-Two-Port Media Access Control Relay (TPMR) group address

Default

By default, lacp destination-mac is multicast-group-address

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#config terminal
(config)#interface eth1
(config-if)#lacp destination-mac customer-bridge-group-address
```

lacp force-up

Use this command to make a port immediately begin forwarding packets and not wait for an LACPDU. After you execute this command, the member port is forcefully up even if LACP is not in sync (only if no other member in the aggregator is in sync).

If a force-up port stops receiving LACPDUs, the port ignores the time-out and remains in operation.

This command can be configured on one member interface of a port channel.

Note: This command can only be given after executing the channel-group mode command on an interface. Force-up mode is not supported for LACP passive mode.

Note: For MLAG, only configure a force-up port on either on the master node or the slave node to prevent traffic drops/loops.

Use the `no` form of this command to disable force-up mode.

Command Syntax:

```
lacp force-up
no lacp force-up
```

Parameters

None

Default

By default, LACP force-up mode is disabled.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#channel-group 1 mode active
(config-if)#lacp force-up
(config-if)#exit
```

lacp port-priority

Use this command to set the priority of a channel. Channels are selected for aggregation based on their priority with the higher priority (numerically lower) channels selected first.

Use the `no` parameter with this command to set the priority of port to the default value (32768).

Command Syntax

```
lacp port-priority <1-65535>
no lacp port-priority
```

Parameters

`<1-65535>`	Specify the LACP port priority.

Default

By default, lacp port priority is 32768

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#lacp port-priority 34
```

lacp system-priority

Use this command to set the LACP system priority. This priority determines the system responsible for resolving conflicts in the choice of aggregation groups.

Note: A lower numerical value has a higher priority.

Use the `no` parameter with this command to set the system priority to its default value (32768).

Command Syntax

```
lacp system-priority <1-65535>
no lacp system-priority
```

Parameters

`<1-65535>`	System priority.

Default

By default, system priority is 32768

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#lacp system-priority 6700
```

lacp timeout

Use this command to set either a short or long timeout value on a port. The timeout value is the number of seconds before invalidating a received LACP data unit (DU).

Command Syntax

```
lacp timeout (short|long)
```

Parameters

`short`	LACP short timeout. 3 seconds.
`long`	LACP long timeout. 90 seconds.

Note: Short: With this mode, BPDU will be sent at Fast_Periodic_Time of 1 second interval. It will timeout, before invalidating received LACPDU, after 3xFast_Periodic_Time(3seconds),

Long: With this mode, BPDU will be sent at Slow_Periodic_Time of 30 seconds intervals. It will timeout, before invalidating received LACPDU, after 3xSlow_Periodic_Time(90seconds)

Default

By default, lacp timeout is long.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following sets the LACP short timeout on a port.

```
#configure terminal
(config)#interface eth0
(config-if)#lacp timeout short

#configure terminal
(config)#interface eth0
(config-if)#lacp timeout long
```

port-channel min-links

Use this command to set the minimum number of aggregated links that need to be up in the LAG interface.

When a the minimum number of links are configured for a LAG, if the active links for that interface become less than the configured value, then the whole LAG is brought down. When the number of active links become the same or more than the configured value, then the whole LAG is restored.

Use the `no` form of this command to remove the minimum number of aggregated links that need to be up in the LAG interface.

Note:

- The minimum number of aggregated links should be same across both ends of an aggregation interface. If not configured, then on one of the nodes the LAG port will be treated as up and on the other as down and traffic will be discarded.
- When a LAG port is moved to the down state because it does not have the minimum number of required links up and running, then the traffic on the remaining interfaces in the LAG will be counted as port-block discards.
- While configuring min-links, it is recommended to configure PO (LACP) min-links only on one end of an etherchannel because it is specific to the each other and triggers fail-over. The fail-over depends on the mux state and lacp timeout.

Command Syntax

```
port-channel min-links <2-32>
no port-channel min-links
```

Parameters

`<2-32>`	Minimum number of links

Default

By default, port channel min-link is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface po1
(config-if)#port-channel min-links 10
(config-if)#exit
```

port-channel weight

Use this command to configure weighted load balancing on port-channel member links. As per the weights configured, traffic distribution will be happening across the member interfaces.

Consider if ports xe1 and xe2 associated with the L2 lag, having default load-balance as src-dst-mac and by default, best traffic distribution can happen upto 50% on each link (by varying source and destination macs). After weight configured as 2 on interface xe1, the best traffic distribution can happen as 66.66% and 33.33% on xe1 and xe2 respectively.

Note: Maximum weights configured over member interfaces should not cross the maximum member supported under a LAG as per device capacity.

Command Syntax

```
port-channel weight <1-64>
port-channel weight <1-16>
no port-channel weight
```

Parameters

<1-64>	Load balance weight for the interface for the Qumran1 series platforms.
<1-16>	Load balance weight for the interface for the Qumran2 series platforms.

Default

Disabled

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.1.

Example

Static lag:

```
#configure terminal
(config)#interface sa1
(config)#exit
(config)#interface xe2
(config-if)#static-channel-group 1
(config-if)#port-channel-weight 2
(config-if)#exit
(config)#Interface xe3
(config-if)#static-channel-group 1
```

Dynamic lag:

```
#configure terminal
(config)#interface po1
```

```
(config)#exit
(config)#interface xe2
(config-if)#channel-group 1 mode active
(config-if)#port-channel-weight 3
```

show debugging lacp

Use this command to display the status of the debugging of the LACP system.

Command Syntax

```
show debugging lacp
```

Parameters

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show debugging lacp

LACP debugging status:
LACP timer debugging is on
```

show etherchannel

Use this command to display information about link aggregation groups.

Command Syntax

```
show etherchannel
show etherchannel <1-16383>
```

With MLAG:

```
show etherchannel (<1-16383>|) detail
show etherchannel (<1-16383>|) limit
show etherchannel (<1-16383>|) load-balance
show etherchannel (<1-16383>|) summary
```

Without MLAG:

```
show etherchannel (<1-16383>|) detail
show etherchannel (<1-16383>|) limit
show etherchannel (<1-16383>|) load-balance
show etherchannel (<1-16383>|) summary
```

Parameters

`<1-16383>`	Specify channel-group number.
`detail`	Specify detailed etherchannel information.
`limit`	Specify channel limit.
`Max Aggregators`	Maximum number of aggregators supported is 128.
`Max Ports in Aggregator`	Maximum number of ports supported in aggregator 16.
`load-balance`	Specify load balancing.
`summary`	Specify Etherchannel summary information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
OcNOS#show etherchannel limit
Max Aggregators         : 256
Max Ports in Aggregator : 64

OcNOS#show etherchannel summary
% Aggregator po1 185
% Aggregator Type: Layer3
% Admin Key: 0001 - Oper Key 0001
%   Link: eth3 (5) sync: 0
```

```
-------------------------------------
% Aggregator po4 186
% Admin Key: 0004 - Oper Key 0004
%   Link: eth2 (4) sync: 0
-------------------------------------
% Aggregator po5 187
% Admin Key: 0005 - Oper Key 0005
%   Link: eth1 (3) sync: 0


OcNOS#show etherchannel detail
% Aggregator po1 185
% Aggregator Type: Layer3
%  Mac address: 08:00:27:36:f5:7d
%  Admin Key: 0001 - Oper Key 0001
%  Actor LAG ID- 0x8000,08-00-27-fa-4b-0e,0x0001
%  Receive link count: 0 - Transmit link count: 0
%  Individual: 0 - Ready: 0
%  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
%   Link: eth3 (5) sync: 0
%  Collector max delay: 5
-------------------------------------------------
% Aggregator po4 186
%  Mac address: 08:00:27:76:0c:57
%  Admin Key: 0004 - Oper Key 0004
%  Actor LAG ID- 0x8000,08-00-27-fa-4b-0e,0x0004
%  Receive link count: 0 - Transmit link count: 0
%  Individual: 0 - Ready: 1
%  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
%   Link: eth2 (4) sync: 0
%  Collector max delay: 5
-------------------------------------------------
% Aggregator po5 187
%  Mac address: 08:00:27:2f:d5:ae
%  Admin Key: 0005 - Oper Key 0005
%  Actor LAG ID- 0x8000,08-00-27-fa-4b-0e,0x0005
%  Receive link count: 0 - Transmit link count: 0
%  Individual: 0 - Ready: 0
%  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
%   Link: eth1 (3) sync: 0
%  Collector max delay: 5
```

Table 5-17 explains the show command output fields.

Table 5-17: show etherchannel detail output

Field	Description
Aggregator	Link aggregators name and ID number.
Mac address	Unique MAC address for link identification.
Admin Key	LACP administrative key – automatically configured value on each port configured to use LACP.
Oper Key	LACP operator key on Partner – automatically configured value on each port configured to use LACP.

Table 5-17: show etherchannel detail output (Continued)

Field	Description
Actor LAG ID	LAG ID consisting of MAC address plus aggregator ID number for this Actor.
Receive link count	The number of link received from the peer LAG.
Transmit link count	The number of links contained transmitted to the peer LAG.
Individual	The individual physical network interfaces or ports contained in the LAG.
Ready	The number of links in the active state on this Actor.
Partner LAG ID	Partner LAG ID consisting of MAC address plus aggregator ID number.
Link	Interface and ID number of the link.
sync	MAC address synchronization enables a MLAG Partner to forward Layer 3 packets arriving on this interfaces with either its own MAC address or its Partner's.
Collector max delay	Maximum period of wait time between sending of two subsequent Ethernet frames on a link.

show lacp sys-id

Use this command to display the LACP system identifier and priority.

Command Syntax

```
show lacp sys-id
```

Parameters

`sys-id`	Display LACP system ID and priority

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show lacp sys-id
% System 8000,00-0e-0c-83-37-27
```

show lacp-counter

Use this command to display the packet traffic on all ports of all present LACP aggregators, or a given LACP aggregator.

Command Syntax

```
show lacp-counte
show lacp-counter <1-16383>
```

Parameters

<1-16383>	Channel-group number

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show lacp-counter 555

Port      LACPDUs          Marker          Pckt err
        Sent    Recv    Sent    Recv    Sent    Recv
```

show port etherchannel

Use this command to display details about a PO and its members' interfaces or to display details of a single member interface of a PO.

Command Syntax

```
show port etherchannel IFNAME
```

Parameters

IFNAME	Interface name

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show port etherchannel ce29/1
LAG ID                        : 0x8000,cc-37-ab-a0-89-ca,0x0002
Partner oper LAG ID           : 0x8000,a8-2b-b5-38-1e-48,0x0004
Aggregator ID                 : 100002
  LACP link info              : ce29/1 - 10001
  Periodic Transmission
  machine state               : Slow periodic
  Receive machine state       : Current
  Mux machine state           : Collecting/Distributing
  Actor Info :
  ===========
  Actor Port priority         : 0x8000 (32768)
  Admin key                   : 0x0002 (2) Oper key: 0x0002 (2)
  Physical admin key          : (2)
  Actor Oper state            : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
  Actor Admin state           : ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
  Partner Info:
  ============
  Partner oper port           : 10009
  Partner link info           : admin port 0
  Partner admin LAG ID        : 0x0000-00:00:00:00:0000
  Partner system priority     : admin:0x0000 - oper:0x8000
  Partner port priority       : admin:0x0000 - oper:0x8000
  Partner oper state          : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
  Partner admin state         : ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0


#show port etherchannel po2
LAG ID                        : 0x8000,cc-37-ab-a0-89-ca,0x0002
Partner oper LAG ID           : 0x8000,a8-2b-b5-38-1e-48,0x0004
Aggregator ID                 : 100002
  LACP link info              : ce29/1 - 10001
  Periodic Transmission
  machine state               : Slow periodic
```

```
Receive machine state      : Current
Mux machine state          : Collecting/Distributing
Actor Info :
===========
Actor Port priority        : 0x8000 (32768)
Admin key                  : 0x0002 (2) Oper key: 0x0002 (2)
Physical admin key         : (2)
Actor Oper state           : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Actor Admin state          : ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
Partner Info:
============
Partner oper port          : 10009
Partner link info          : admin port 0
Partner admin LAG ID       : 0x0000-00:00:00:00:0000
Partner system priority    : admin:0x0000 - oper:0x8000
Partner port priority      : admin:0x0000 - oper:0x8000
Partner oper state         : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Partner admin state        : ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0

LACP link info             : ce30/1 - 10005
Periodic Transmission
machine state              : Slow periodic
Receive machine state      : Current
Mux machine state          : Collecting/Distributing
Actor Info :
===========
Actor Port priority        : 0x8000 (32768)
Admin key                  : 0x0002 (2) Oper key: 0x0002 (2)
Physical admin key         : (2)
Actor Oper state           : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Actor Admin state          : ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
Partner Info:
============
Partner oper port          : 10013
Partner link info          : admin port 0
Partner admin LAG ID       : 0x0000-00:00:00:00:0000
Partner system priority    : admin:0x0000 - oper:0x8000
Partner port priority      : admin:0x0000 - oper:0x8000
Partner oper state         : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
Partner admin state        : ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
```

Note: Most of the output of this command is duplicated in the show etherchannel command (see also the 802.3ad specification). The output of the `show port etherchannel` command is primarily a list of state machine values. An explanation of the state machine bits follows. See Figure 5-52.

Table 5-18 explains the show command output fields.

Table 5-18: show port etherchannel detailed output

Entry	Description
Actor/Partner state	The Actor's and Partner's state variables, encoded as individual bits within a single octet.
ACT	LACP_Activity is encoded in bit 0. Active LACP is encoded as a 1; Passive LACP as a 0.

Table 5-18: show port etherchannel detailed output (Continued)

Entry	Description
TIM	LACP_Timeout is encoded in bit 1. Short Timeout is encoded as a 1; Long Timeout as a 0.
AGG	Aggregability is encoded in bit 2. Aggregatable is encoded as a 1; Individual is encoded as a 0.
SYN	Synchronization is encoded in bit 3. In_Sync is encoded as a 1; Out_Of_Sync is encoded as a 0.
COL	Collecting is encoded in bit 4. True is encoded as a 1; False is encoded as a 0.
DIS	Distributing is encoded in bit 5. True is encoded as a 1; False is encoded as a 0.
DEF	Defaulted is encoded in bit 6.
EXP	Defaulted is encoded in bit 7.

Bits 7 and 8 are reserved; these are ignored on receipt and transmitted as zero. However, the received value of these bits is recorded on receipt to accurately reflect the actor's view of the partner's state in outgoing PDUs.

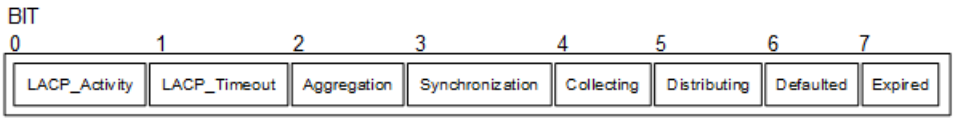


Figure 5-52: Diagram of state machine octet

show static-channel-group

Use this command to display the types of load-balancing port selection criteria (PSC) used on configured static aggregators.

Command Syntax

```
show static-channel-group(<1-16383>|)
```

Parameters

<1-16383>	Specify channel-group number.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following is an example of the output of this command:

```
#show  static-channel-group 1
% Static Aggregator: sa1
% Member:
   eth1
```

show static-channel load-balance

Use this command to display information about static channel groups.

Command Syntax

```
show static-channel (<1-16383>|) load-balance
```

Parameters

<1-16383>	Specify static-channel-group number.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS Version 1.0.

Examples

The following is an example of the output of this command:

```
#show static-channel load-balance
% Static Aggregator: sa5
Flow based division
```

snmp restart lacp

Use this command to restart SNMP in LACP.

Command Syntax

```
snmp restart lacp
```

Parameters

None

Default

By default, snmp restart lacp is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#snmp restart lacp
```

static-channel-group

Use this command to create a static link aggregation group or to add an interface to an existing link aggregation group.

Use the `no` form of this command to remove an interface from a static link aggregation group without removing the static link aggregation group itself.

Command Syntax

```
static-channel-group <1-16383>
no static-channel-group
```

Parameter

`<1-16383>`	Channel group number.

Default

By default, static channel group is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#static-channel-group 1
(config-if)#exit

#sh run in sa1
!
interface sa1
 switchport
```

This is an example of `no static-channel-group`:

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#no static-channel-group
(config-if)#exit

#sh run in xe1
!
interface xe1 switchport
!
#sh run in sa1
!
interface sa1
 switchport
!
```

CHAPTER 6 Multi-chassis Link Aggregation Commands

This chapter describes the Multi-Chassis Link Aggregation commands.

Multi-Chassis Link Aggregation is also called MC-LAG, MLAG, or Distributed Resilient Network Interconnect (DRNI). In this document, it is called MLAG.

clear mcec statistics

Use this command to clear the statistics related to hello and information PDUs in the MCEC domain.

Command Syntax

```
clear mcec statistics
```

Parameters

None

Command Mode

Privileged exec mode

Applicability

This command was introduced before OcNOS version 4.0.

Examples

```
#clear mcec statistics
```

domain-address

Use this command to configure domain address, which helps to identify the mcec domain.

Use the `no` form of this command to remove the domain address.

Command Syntax

```
domain-address <domain-id>
no domain-address
```

Parameters

```
domain-id  domain address in HHHH.HHHH.HHHH format
```

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#domain-address 1111.2222.3333
```

debug mcec

Use this command to view debugging logs for MLAG.

Use the `no` form of this command to remove debugging logs for MLAG.

Command Syntax

```
debug mcec (timer|event|hello|info|cli|mac-sync|all)
no debug mcec (timer|event|hello|info|cli|mac-sync|all)
```

Parameters

`all`	ALL
`cli`	CLI
`event`	Event
`hello`	Hello
`info`	Info
`mac-sync`	Mac Sync
`timer`	Timer

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug mcec all
#no debug mcec all
```

domain hello timeout

Use this command to specify the domain hello-timeout value.

Command Syntax

```
domain-hello-timeout (long|short)
no domain-hello-timeout
```

Parameters

`long`	Long Timeout
`short`	Short Timeout

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#domain-hello-timeout long
```

domain priority

Use this command to specify the priority value associated with mcec domain.

Use the `no` form of this command to remove the priority value associated with mcec domain.

Command Syntax

```
domain-priority <1-65535>
no domain-priority
```

Parameters

`<1-65535>`	Priority Value

Default

The default value is 32768.

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#domain-priority 2
```

domain-system-number

Use this command to configure domain system number, which uniquely identifies domain system in mcec domain.

Use the `no` form of this command to configure domain system number.

Command Syntax

```
domain-systm-number <1-2>
no domain-systm-number
```

Parameters

`<1-2>`	Domain System Number

Command Mode

MLAC mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#domain-system-number 2
```

intra-domain-link

Use this command to map an interface as intra domain link that connects the domain system with its neighbor in a mcec domain.

Use the no form of this command to unmap the interface configured as intra domain link that connects the domain system with its neighbor in a mcec domain.

Command Syntax

```
intra-domain-link <IFNAME>
no intra-domain-link
```

Parameters

IFNAME	Interface name

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#intra-domain-link eth2
```

intra-domain-peer

Use this command to map an interface as intra domain peer that connects the domain system with its neighbor in a mcec domain.

Use the `no` form of this command to unmap the interface configured as intra domain peer that connects the domain system with its neighbor in a mcec domain.

Command Syntax

```
intra-domain-peer A.B.C.D source-address A.B.C.D (vrf VRF_NAME|)
no intra-domain-peer
```

Parameters

`Peer Address`	Peer/Target IPv4 address
`A.B.C.D`	IPv4 address.
`source-address`	Source IPv4 address
`A.B.C.D`	IPv4 address.
`VRF_NAME`	VRF Interface name

Command Mode

MCEC mode

Applicability

This command was introduced before OcNOS version 3.0.

Example

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#intra-domain-peer 1.1.1.1 source-address 2.2.2.2 vrf
myvrf
```

mcec domain configuration

Use this command to enter MCEC Domain configuration mode to configure mcec domain information.

Command Syntax

```
mcec domain configuration
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#
```

mcec strict-active-standby

Use this command to control strict Active-Standby behavior for Dynamic MLAG (Mlag-Po) interfaces.

Note:

- This command can be configured only when a single communication channel exists between MLAG Primary and Secondary nodes (either IDL or IDP).
- This command applies only to Dynamic Active-Standby MLAG (Mlag-Po) interfaces.
- The configuration takes effect on the next Domain Adjacency DOWN event.

Case 1: Strict Active-Standby Enabled (Default)

When Domain Adjacency goes DOWN (IDL/IDP link failure):

MLAG nodes remain in strict Active-Standby mode; only one node (Primary or Secondary) is Active.This prevents a split-brain (Active-Active) condition that could cause network disruption.

When the Active MLAG node reboots:

If the reboot occurs via OcNOS commands, the Standby node becomes Active.

If the reboot occurs for any other reason (power failure, APC reboot, admin reboot from Linux prompt, node crash), the Standby node remains in Standby, resulting in 100% traffic loss until the Active node recovers.

Case 2: Strict Active-Standby Disabled

When Domain Adjacency goes DOWN (IDL/IDP link failure):

Both Primary and Secondary nodes' MLAG Active-Standby interfaces become Active.This produces a split-brain (Active-Active) condition; network disruption is expected.

When the Active MLAG node reboots:

If the reboot occurs via OcNOS commands, the Standby node becomes Active.

If the reboot occurs for any other reason (power failure, APC reboot, admin reboot from Linux prompt, node crash), the Standby node's MLAG Active-Standby interfaces become Active, preventing significant traffic loss.

Command Syntax

```
mcec strict-active-standby disable
no mcec strict-active-standby
```

Parameters

disable	Disables strict Active-Standby behavior.

Default

Enabled

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.5.2.

Examples

```
# configure terminal
(config)# mcec strict-active-standby disable

# Re-enable default strict Active-Standby
(config)# no mcec strict-active-standby
```

mlag

Use this command to create mlag instance.

Note: The mlag interface must be associated to a port channel.

Note: All MLAG nodes must use the same MAC table size.

Use the `no` form of this command to un-map the mlag instance.

Command Syntax

```
mlag <1-256>
no mlag
```

Parameters

`<1-256>`	MLAG identifier

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 4.1.

Example

```
#config terminal
(config)#interface mlag1
```

mode

Use this command to set the MLAG mode.

Use the `no` form of this command to turn off this feature.

Command Syntax

```
mode (active-standby|active-active)
no mode (active-standby|active-active)
```

Parameters

`active-standby`	The interface is ready for transition to the active state if a failure occurs in the other node.
`active-active`	The interface is the active interface that carries the traffic.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 4.0.

Examples

```
(config)#
(config)#interface mlag1
(config-if)#mode active-standby
```

show mcec statistics

Use this command to display all the statistics related to hello and info pdu's in mcec domain.

Command Syntax

```
show mcec statistics
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sh mcec statistics
Unknown MCCPDU received on the system : 0

-----------------------------------
IDP xe49
-----------------------------------
Valid RX Hello PDUs : 109
Valid TX Hello PDUs : 201
Valid RX Info PDUs: 23
Valid TX Info PDUs : 28
Valid RX Mac Sync PDUs : 5
Valid TX Mac Sync PDUs : 4

MLAG 1
Valid RX Info PDUs : 5
Valid TX Info PDUs : 7
```

Table 6-19 Shows the output details.

Table 6-19: Show mcec statistics details

Entry	Description
RX Hello PDUs	Total number of received hello PDUs.
TX Hello PDUs	Total number of transmitted hello PDUs.
RX Info PDUs	Total number of received Info PDUs.
TX Info PDUs	Total number of transmitted Info PDUs.
RX Mac Sync PDUs	Total number of received Mac Sync PDUs.
TX Mac Sync PDUs	Total number of transmitted Mac Sync PDUs.

show mlag detail

Use this command to display details about MLAG configuration and status.

Command Syntax

```
show mlag <1-256> detail
```

Parameters

<1-256>	MLAG group number

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sh mlag 1 detail

MLAG-1
Mapped Aggregator : po1
Admin Key : 32769
Oper Key: 16385
Physical properties Digest : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

Neigh Admin Key: 16385
Neigh Physical Digest: dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
Info RCV State : Current
Info Periodic Time State : Standby
Mlag Sync: IN_SYNC
```

Table 6-20 Shows the output details.

Table 6-20: Show mlag output details

Entry	Description
Mapped Aggregator	Map the output of the aggregator in the interface which is active transformation.
Admin Key	MLAG administrative key – automatically configured value on each port configured to use MLAG.
Oper Key	MLAG operator key on Partner – automatically configured value on each port configured to use MLAG.
Physical properties Digest	Physical properties of the digest.
Neigh Admin Key	Neigh administrative key – automatically configured value on each port configured to use MLAG.
Neigh Physical Digest	Neigh physical properties of the digest.

Table 6-20: Show mlag output details

Entry	Description
Info RCV State	Details of the RCV.
Info Periodic Time State	A simple state space formulation of a general digital periodic time series is constructed.
Mlag Sync	MAC address synchronization enables a MLAG Partner to forward Layer 3 packets arriving on this interfaces with either its own MAC address or its Partner's.

show mlag domain

Use this command to display MLAG configuration and status.

Command Syntax

```
show mlag domain <details|summary>
```

Parameters

`details`	details
`summary`	summary

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show mlag domain summary
-----------------------------------
Domain Configuration
-----------------------------------
Domain System Number : 2
Domain Address: 1111.2222.3333
Domain Priority: 1000
Intra Domain Interface: xe49
Domain Adjacency: UP

-----------------------------------
MLAG Configuration
-----------------------------------

MLAG-1
Mapped Aggregator: po1
Physical properties Digest: dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
Total Bandwidth : 40g
Mlag Sync : IN_SYNC


#sh mlag domain details
-----------------------------------
Domain Configuration
-----------------------------------

Domain System Number: 2
Domain Address: 1111.2222.3333
Domain Priority: 1000
Intra Domain Interface: xe49

Hello RCV State: Current
Hello Periodic Timer State: Fast Periodic
```

```
Domain Sync : IN_SYNC
Neigh Domain Sync : IN_SYNC
Domain Adjacency : UP

-----------------------------------
MLAG Configuration
-----------------------------------

MLAG-1
Mapped Aggregator: po1
Admin Key: 32769
Oper Key: 16385
Physical properties Digest: dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

Neigh Admin Key: 16385
Neigh Physical Digest : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
Info RCV State : Current
Info Periodic Time State : Standby
Mlag Sync : IN_SYNC
```

Table 6-21 Shows the output details.

Table 6-21: Show mlag summary details

Entry	Description
Domain System Number	Number to identify the node in domain.
Domain Address	Domain address for the MLAG domain.
Domain Priority	Domain priority for the MLAG domain.
Intra Domain Interface	Intra domain interface between MLAG domains.
Domain Adjacency	Domain adjacency details and configuration.
Physical properties Digest	physical properties of the digest algorithm.
Total Bandwidth	Total bandwidth available on the interface.
Domain System Number	Number of the domain system.
Domain Address	Domain address for the MLAG domain.
Domain Priority	Domain priority for the MLAG domain.
Intra Domain Interface	Details of the intra domain in the interface.
Hello RCV State	State of the hello RCV in the interface.
Hello Periodic Timer State	State of the hello periodic timer in the interface.
Domain Sync	Detail of the domain configuration synchronization.
Mapped Aggregator	Map the output of the aggregator in the interface which is active transformation.
Admin Key	MLAG administrative key – automatically configured value on each port configured to use MLAG.

Table 6-21: Show mlag summary details

Entry	Description
Oper Key	MLAG operator key on Partner – automatically configured value on each port configured to use MLAG.
Physical properties Digest	Physical properties of the digest.
Neigh Admin Key	Neigh administrative key – automatically configured value on each port configured to use MLAG.
Neigh Physical Digest	Neigh physical properties of the digest.
Info RCV State	Details of the RCV.
Info Periodic Time State	A simple state space formulation of a general digital periodic time series is constructed.
Mlag Sync	MAC address synchronization enables a MLAG Partner to forward Layer 3 packets arriving on this interfaces with either its own MAC address or its Partner's.

show mlag stp-synchronization status

Use this command to display information about MLAG STP Syncronization status

Command Syntax

```
show mlag stp-synchronization status
```

Parameters

`stp-synchronization`	STP synchronization related show commands
`status`	STP synchronization status

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show mlag stp-synchronization status

 Home STP Domain Digest     : 27 e7 22 79 76 b2 c8 4e 49 9f b4 45 4f 20 68 aa
 Neighbor STP Domain Digest : 27 e7 22 79 76 b2 c8 4e 49 9f b4 45 4f 20 68 aa
 STP Sync Status            : IN_SYNC

-----------------------------------------------------

 MLAG Interface Status:

 MLAG1:

  Home Interface Digest       : 76 88 b9 cd 43 c1 b0 9d b 86 64 e5 b7 d2 7f a7
  Neighbor Interface Digest   : 76 88 b9 cd 43 c1 b0 9d b 86 64 e5 b7 d2 7f a7
  STP Sync Status             : IN_SYNC
#

Entry                                   Description
Home STP Domain Digest                 STP Domain properties of the digest
Neighbor STP Domain Digest             Neighbor STP Domain properties of the
digest
STP Sync Status                        Detail of configurated STP
synchronization.
Home Interface Digest                  Interface properties of the digest.
Neighbor Interface Digest              Neigh Interface properties of the
digest.
```

show spanning-tree mlag operational-config

Use this command to display the operational information for MLAG.

Command Syntax

```
show spanning-tree mlag operational-config
```

Parameters

None

Command Mode

Privilege exec mode

Applicability

This command was introduced before OcNOS version 4.0.

Examples

```
#show spanning-tree mlag operational-config
Operational Configuration
----------------------------------------
Bridge Priority : 32768
Pathcost method : Long
Interface : mlag1
Pathcost : 1000
Priority : 0
```

show spanning-tree mlag sync-detail

Use this command to display the spanning-tree properties shared with the domain peer node.

Command Syntax

```
show spanning-tree mlag sync-detail
```

Parameters

None

Command Mode

Privilege exec mode

Applicability

This command was introduced before OcNOS version 4.0.

Examples

```
#show spanning-tree mlag sync-detail
Domain Digest Parameters
----------------------------------------
Max Age : 20
BPDU Filter : Disabled
BPDU Guard : Disabled
Hello time : 2
Forward Delay : 15
Force Version : 2
Err-disable status : Disabled
Err-disable timeout : 300
MSTP Enabled : Enabled
MSTP Bridge Forward : Disabled
Interface Digest parameters
----------------------------
Port Name : mlag1
Admin Root Guard : Disabled
Admin Edge port : Disabled
Portfast configuration : Disabled
Restricted TCN : Disabled
Admin BPDU filter : Default
Admin BPDU guard : Default
```

switchover type

Use this command to set the MLAG switchover type.

Use the `no` form of this command to turn off switchover.

Command Syntax

```
switchover type revertive <1-3600>
switchover type non-revertive
no switchover type (revertive | non-revertive)
```

Parameters

`revertive <1-3600>`	A network failure triggers a switchover, the initially active node becomes active again after failure recovery. Configure the number of seconds within this range to switch back to the initially active node after the failure recovery. The default time is 10 seconds.
`non-revertive`	A network failure triggers a switchover, the initially active node remains on standby after failure recovery.

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 4.0 and the `revertive <1-3600>` is revised in OcNOS version 6.6.0.

Examples

```
OcNOS(config)#interface mlag1
OcNOS(config-if)#switchover type revertive 20

OcNOS(config)#interface mlag1
OcNOS(config-if)#switchover type non-revertive
```

CHAPTER 7 Traffic Mirroring Commands

This chapter provides a description of syntax, and examples for Traffic Mirroring. It includes the following commands:

monitor session

Use this command to create a local or remote monitor session. By default, a local monitor session is created.

A monitor session consists of:

- A single destination interface, referred to as a mirror-to port or a single remote destination
- One or more source interfaces (egress, ingress, or both)
- One or more VLAN sources in the ingress direction
- One or more filters that can be applied to filter the mirrored packets

Use the `no` parameter to delete a monitor session.

Command Syntax

```
monitor session <1-18> ( | type ( local | remote ))
no monitor session ( <1-18> | all )
```

Parameters

`<1-18>`	Session number
`local`	Create a local session
`remote`	Create a remote source node session
`all`	All sessions

Default

By default, monitor session type is local and will not be active by default

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#monitor session 1
(config-monitor)#exit
(config)#monitor session 3 type remote
(config-monitor)#exit
(config)#no monitor session 1
```

monitor session shut

Use this command to deactivate one monitor session.

Use the `no` parameter to activate one monitor session.

Command Syntax

```
monitor session <1-18> shut
no monitor session <1-18> shut
```

Parameters

`<1-18>`	Session number

Default

Monitor session will not be active by default

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#monitor session 3 shut

(config)#no monitor session 3 shut
```

source interface

Use this command to configure a source port per monitor session in either ingress or egress or both directions. Source port can be physical interface or a trunk port.

Use the `no` parameter to remove the source port.

Note: The behavior is changed when the configuration is edited in the current release: For example, if you have configured as follows

```
source interface xe10 rx → running-config/backend: source interface xe10 rx
source interface xe10 tx → running-config/backend: source interface xe10 both
```

its direction is changed to as follows

```
source interface xe10 rx → running-config/backend: source interface xe10 rx
source interface xe10 tx → running-config/backend: source interface xe10 tx
```

Command Syntax

```
source interface IFNAME ( rx | tx | both | )
no source interface IFNAME
```

Parameters

`IFNAME`	Interface name
`rx`	Ingress direction
`tx`	Egress direction
`both`	Both directions

Default

Source port will be mirrored for both directions if the direction is not specified

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 1
(config-monitor)#source interface xe1 both
(config-monitor)#no source interface xe1
```

source vlan

Use this command to configure one or more VLANs as source per monitor session. A VLAN as source will be mirrored only in the ingress direction. Up to 32 VLANs can be configured as source per monitor session.

Use the `no` parameter to remove vlan source from monitor session.

Note: To add or update or delete source VLAN in monitor session, session needs to be in shut state.

Command Syntax

```
source vlan VLAN_RANGE
no source vlan VLAN_RANGE
```

Parameters

`VLAN_RANGE`	VLAN identifier or VLAN identifier range

Default

A trunk port is a member of all VLANs by default.

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 1
(config-monitor)#source vlan 2
(config-monitor)#source vlan 4-10
(config-monitor)#no source vlan 2-5,10
```

destination interface

Use this command to configure a mirror-to port per local monitor session. A destination port can be a physical port or a trunk port.

Use the `no` parameter to remove the destination port from a local monitor session.

Note: For the monitor sessions, the destination interface should be an switchport with no service attached. This port will not participate in L2/L3 packet forwarding.

Command Syntax

```
destination interface IFNAME
no destination interface IFNAME
```

Parameters

`IFNAME`	Interface name

Default

No default value is specified

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe3
(config-if)#switchport
(config-if)#exit
(config)#monitor session 1
(config-monitor)#destination interface xe3
(config-monitor)#no destination interface xe3
```

no shut

Use this command to activate a monitor session

Command Syntax

```
no shut
```

Parameters

None

Default

Monitor session will not be active by default.

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#no shut
```

shut

Use this command to de-activate a monitor session.

Command Syntax

```
shut
```

Parameters

None

Default

Monitored session is not active by default.

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#shut
```

filter

Use this command to add filters to the monitor session. Filters can be applied only in case of ingress mirroring. The configuration of sequence identifier for each rule is optional, but even if it is not configured explicitly, it will always be generated and in steps of 10.

Use the `no` parameter to remove the filter from monitor session.

Note: To add or update or delete any filters in monitor session, session needs to be in shut state.

Command Syntax

```
(<1-268435453>/<1-4294967294> |) filter {vlan VLAN_RANGE| cos <0-7> | dest-mac
  (host XXXX.XXXX.XXXX | XXXX.XXXX.XXXX XXXX.XXXX.XXXX) | src-mac (host
  XXXX.XXXX.XXXX | XXXX.XXXX.XXXX XXXX.XXXX.XXXX) | frame-type (ETHTYPE | arp (req
  | resp|) (sender-ip A.B.C.D|) (target-ip A.B.C.D|) | ipv4 (src-ip (A.B.C.D |
  A.B.C.D/M)|) (dest-ip (A.B.C.D | A.B.C.D/M)|) | ipv6 (src-ip X:X::X:X/M |) (dest-
  ip X:X::X:X/M |))}
no (<1-268435453>/<1-4294967294>) filter
```

Parameters

(<1-268435453>/<1-4294967294> |)	Sequence identifier for each rule.
<2-4094>	VLAN identifier
<0-7>	COS number
XXXX.XXXX.XXXX	MAC address
ETHTYPE	Ethertype
arp	ARP frames
req	Request frames
resp	Response frames
A.B.C.D	Single IP address
A.B.C.D/M	IP addresses with mask
X:X::X:X/M	IPv6 addresses with mask

Default

No default value is specified.

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#filter dest-mac host 0000.0001.2421 frame-type ipv4
```

```
(config-monitor)#filter cos 3 frame-type arp req sender-ip 2.2.2.1
(config-monitor)#35 filter vlan 200
(config-monitor)#no 10 filter
(config-monitor)#no 20 filter
(config-monitor)#no 35 filterr
```

description

Use this command to add a description to the monitor session.

Use the `no` parameter to delete a description of the monitor session.

Command Syntax

```
description LINE
no description
```

Parameters

`LINE`	Enter the description string

Default

No default value is specified.

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#description “port mirror rx”
(config-monitor)#no description
```

remote destination

Use this command to configure a destination VLAN and the reflector port for the remote monitor session.

Use the `no` parameter to remove a destination from a remote monitor session.

Command Syntax

```
destination remote vlan <2-4094> reflector-port IFNAME
no destination remote
```

Parameters

`<2-4094>`	VLAN identifier
`IFNAME`	Interface name

Default

No default value is specified

Command Mode

Monitor configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#no vlan 900 bridge 1
(config)#interface xe3
(config-if)#switchport
(config)#monitor session 1
(config-monitor)#destination remote vlan 900 reflector-port xe3
(config-monitor)#no destination remote
```

show monitor

Use this command to display states of all monitor sessions. If a session is down, the reason is displayed.

Command Syntax

```
show monitor
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show monitor
Session   State          Reason               Description
------- ----------- ---------------------- --------------------------------
1       down        No sources configured
2       down        Dst in wrong mode
```

show monitor session

Use this command to display the configuration details of one or more monitor sessions.

Command Syntax

```
show monitor session (<1-18>|all|(range RANGE)) (brief|)
```

Parameters

`<1-18>`	Session number
`all`	All sessions
`RANGE`	Session number range (n1-n2)
`brief`	Brief information

Command Mode

Exec mode or Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show monitor session 1
session 1
---------------
type               : local
state              : down (Session admin shut)
source intf        :
tx                 : xe1 xe3 xe4
rx                 : xe2 xe3 xe4
both               : xe3 xe4
source VLANs       :
rx                 : 2,5-10,15,18-20
destination ports  : xe5
filter count       :

Legend: f = forwarding enabled, l = learning enabled
#
```

Table 7-22 Explains the show command output fields

Table 7-22: Show monitor session output fields

Field	Description
Type	Type of monitor session.
State	State of the security flow filter.
Rx	Incoming flow (source and destination IP addresses).
Tx	Reverse flow (source and destination IP addresses).

Field	Description
Both	Incoming and reverse flow (source and destination IP address)
Destination Port	Name of the destination port to be matched.
Source intf	Number of maximum intf central source session.
Source VLANs	Number of maximum VLANs central source session.
Filter count	Used to count number of lines in a file or table.

show filter

Use this command to display filters for one or more monitor sessions.

Command Syntax

```
show monitor session (<1-18>|all|(range RANGE)) filter
```

Parameters

`<1-18>`	Session number
`all`	All sessions
`RANGE`	Session number range (n1-n2)

Command Mode

Exec mode or Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show monitor session 1 filter
session 1
---------------
filter count : 3
---------------

match set 1
---------------
destination mac address : 0000.0002.4451 (host)
source mac address : 0000.0012.2288 (host)
---------------

match set 2
---------------
frame type : arp
sender ip address : 2.2.2.5
target ip addres : 2.2.2.8
---------------

match set 3
---------------
destination mac address : 0000.0001.1453 (host)
frame type : ipv4
source ip address : 3.3.3.5
#
```

show monitor running configuration

Use this command to display the mirror-related running configuration.

Command Syntax

```
show running-config monitor (all|)
```

Parameters

`all`	Show running configuration with defaults

Command Mode

Exec mode or Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config monitor
!
monitor session 1
 source interface xe10 rx
 destination interface po1
 no shut
#
```

CHAPTER 8 VLAN and Private VLAN Commands

This chapter has the commands used to manage VLANs and Private VLANs. A private VLAN contains switch ports that cannot communicate with each other, but can access other networks. This chapter includes the following commands:

global-bridge-vlan-check enable

Use this command to establish a VLAN in the global VLAN database, ensuring that the same VLAN is not permitted to be encapsulated on a sub-interface.

Command Syntax

```
global-bridge-vlan-check enable
no global-bridge-vlan-check enable
```

Parameters

`enable`	Enable VLAN check validations

Default

Disabled.

Command Mode

VLAN Configuration mode

Applicability

This command is introduced from OcNOS version 6.5.1.

Example

1. Validating sub-interface encap VLANs should not be overlapped with bridge VLANs.

```
#(config)#bridge 1 protocol rstp vlan-bridge
(config)#vlan 2-10 bridge 1
(config)#commit
(config)#
(config)#global-bridge-vlan-check enable
(config)#commit
(config)#
(config)#int xe2.2 switchport
(config-if)#encapsulation dot1q 2
(config-if)#commit
```

Bridge VLAN ids cannot be used for L2 sub-interface's encaps

Failed to commit. As error(s) encountered during commit operation.

2. Configure sub-interface encap VLANs when not overlapping with bridge VLAN IDs.

```
#(config)#int xe5.5 switchport
(config-if)#encapsulation dot1q 11
(config-if)#commit
(config-if)#exit
(config)#end
```

private-vlan association

Use this command to associate a secondary VLAN to a primary VLAN. Only one isolated VLAN can be associated to a primary VLAN. Multiple community VLANs can be associated to a primary VLAN.

Use the `no` form of this command to remove association of all the secondary VLANs to a primary VLAN.

Command Syntax

```
private-vlan association add VLAN_RANGE
private-vlan association remove VLAN_RANGE
no private-vlan association
```

Parameters

`add`	Add a VLAN to private VLAN list.
`remove`	Removes values associated with a single VLAN.
`VLAN_RANGE`	Specify VLAN ID 1-4094 or range(s): 1-5, 10 or 2-5,7-19 of the private VLANs to be configured

Default

By default, functionality is disabled

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan database
(config-vlan)#private-vlan association add 3-4
(config-vlan)#private-vlan association remove 3-4
(config-vlan)#no private-vlan association
```

private-vlan community

Use this command to set a VLAN type for a private (community) VLAN.

Use the `no` form of this command to remove the specified private VLAN.

Command Syntax

```
private-vlan <2-4094> community bridge <1-32>
no private-vlan <2-4094> bridge <1-32>
```

Parameters

`<2-4094>`	Specify a private VLAN identifier.
`bridge`	Specify the bridge identifier.

Default

By default, private vlan is disabled

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan database
(config-vlan)#private-vlan 4 community bridge 1
```

private-vlan isolated

Use this command to create an isolated private VLAN.

Use the `no` form of this command to remove the specified private VLAN.

Command Syntax

```
private-vlan <2-4094> isolated bridge <1-32>
no private-vlan <2-4094> bridge <1-32>
```

Parameters

`<2-4094>`	Specify a private VLAN identifier.
`bridge`	Specify the bridge identifier.

Default

By default, private vlan is disabled

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan database
(config-vlan)#private-vlan 3 isolated bridge 1
```

private-vlan primary

Use this command to create a primary VLAN.

Use the `no` form of this command to remove the specified private VLAN.

Command Syntax

```
private-vlan <2-4094> primary bridge <1-32>
no private-vlan <2-4094> bridge <1-32>
```

Parameters

`<2-4094>`	Specify a private VLAN identifier.
`bridge`	Specify the bridge identifier.

Default

By default, private vlan is disabled

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan database
(config-vlan)#private-vlan 2 primary bridge 1
```

show vlan

Use this command to display information about static, dynamic or all VLANs.

Command Syntax

```
show vlan (all|static|dynamic|auto) bridge <1-32>
```

Parameters

`<1-32>`	Displays the bridge group ID.
`all`	Displays all VLANs (static and dynamic).
`static`	Displays static VLANs.
`dynamic`	Displays dynamic VLANs.
`auto`	Displays auto configured VLANs.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh vlan all bridge 1
Bridge  VLAN ID     Name          State   H/W Status      Member ports
                                                        (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ============================
1       1       default          ACTIVE  Up         xe2(u) xe10(u)
1       2       vlan2            ACTIVE  Up         xe10(t)
1       10      VLAN0010         ACTIVE  Up         xe2(t) xe10(t)
1       20      VLAN0020         ACTIVE  Up         xe2(t) xe10(t)
1       30      VLAN0030         ACTIVE  Up         xe10(t)
1       40      VLAN0040         ACTIVE  Up         xe10(t)
1       50      VLAN0050         ACTIVE  Up         xe10(t)
1       60      VLAN0060         ACTIVE  Up         xe10(t)
#
```

Table 8-23 Explains the show command output fields.

Table 8-23: show vlan output fields

Field	Description
Bridge	Number of bridge in the interface.
VLAN ID	VLAN identifier of the VLAN listed.
Name	Name of the VLAN.
State	Indicates whether the physical link is operational and can pass packets.

Field	Description
H/W Status	Indicates that the hardware is operational.
Member ports	The tagged interfaces to which a VLAN is associated.

show vlan brief

Use this command to display brief VLAN information for all bridges.

Command Syntax

```
show vlan (brief | <2-4094>)
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3. Added the `Total Vlans` field in the command output in OcNOS version 7.0.0.

Example

The following is a sample output from this command.

```
OcNOS#show vlan brief
Bridge  VLAN ID     Name         State   H/W Status      Member ports
                                                        (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
1       1       default          ACTIVE  Success    eth1(u)
1       2       VLAN0002         ACTIVE  Success
1       3       VLAN0003         ACTIVE  Success
1       4       VLAN0004         ACTIVE  Success
1       5       VLAN0005         ACTIVE  Success
1       10      VLAN0010         ACTIVE  Success

Total VLANs: 6
```

Table 8-24 Explains the show command output fields.

Table 8-24: show vlan brief output fields

Field	Description
Bridge	Number of bridge in the interface.
VLAN ID	VLAN identifier of the VLAN listed.
Name	Name of the VLAN.
State	Indicates whether the physical link is operational and can pass packets.
H/W Status	Indicates that the hardware is operational.

Field	Description
Member ports	The tagged interfaces to which a VLAN is associated.
Total VLANs	Displays the total number of VLANs currently configured on the device.

show vlan classifier

Use this command to display information on configured VLAN classifier groups, interfaces configured for a VLAN group or all the groups, or all configured VLAN classifier rules.

If either a group ID or rule ID is not specified, all configured VLAN classifier rules are shown. If either a group ID or rule ID is specified, a specific configured VLAN classifier rule is shown.

Command Syntax

```
show vlan classifier group interface IFNAME
show vlan classifier group (<1-16>|)
show vlan classifier interface group (<1-16>|)
show vlan classifier rule(<1-256>|)
```

Parameters

`group`	Displays group activated information.
`<1-16>`	Displays the group ID
`interface`	Displays interface information.
`interface`	Displays interface group information.
`group`	Displays group activated information.
`<1-16>`	Displays the group ID.
`rule`	Displays VLAN classifier rule ID.
`<1-256>`	Displays rule ID information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example displays groups for VLAN classifier groups:

```
#show vlan classifier group 1
vlan classifier group 1 add rule 1
```

This example displays interfaces for all VLAN classifier groups:

```
#show vlan classifier interface group
vlan classifier group 1 interface fe2
vlan classifier group 1 interface fe3
vlan classifier group 2 interface fe5
vlan classifier group 3 interface fe7
```

This example displays interfaces for VLAN classifier group 1:

```
#show vlan classifier interface group 1
vlan classifier group 1 interface fe2
vlan classifier group 1 interface fe3
```

This example displays interfaces for VLAN classifier rule 1:

```
#show vlan classifier rule 1
vlan classifier rule 1 mac 0011.2222.3333 vlan 2
```

switchport access

Use this command to change the default VLAN on the current interface.

Note: IP Infusion Inc. does not recommend using VLAN identifier 1 because of interoperability issues with other vendors' equipment.

Use the `no` parameter to remove an existing VLAN.

Command Syntax

```
switchport access vlan <2-4094>
no switchport access vlan
```

Parameter

`<2-4094>`	Specify the VLAN identifier.

Default

The switchport access vlan default value is 3968.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows the steps of a typical VLAN session, creating and destroying a VLAN.

```
#configure terminal
(config)#interface eth0
(config-if)#switchport access vlan 3

(config)#interface eth0
(config-if)#no switchport access vlan
```

switchport hybrid

Use this command to set the switching characteristics of the interface to hybrid. Both tagged and untagged frames will be classified over hybrid interfaces.

For a VLAN range, specify two VLAN identifiers: the lowest and then the highest separated by a hyphen. For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces between the hyphens or commas.

Use the `no` parameter to turn off allowed hybrid switching.

Command Syntax

```
switchport hybrid allowed vlan all
switchport hybrid vlan <2-4094>
switchport hybrid allowed vlan none
switchport hybrid allowed vlan remove VLAN_ID
switchport hybrid allowed vlan add VLAN_ID
no switchport hybrid
no switchport hybrid vlan
```

Parameters

`all`	Allow all VLANs to transmit and receive through the interface.
`none`	Allow no VLANs to transmit and receive through the interface.
`remove`	Remove these VLANs from the member set.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.
`add`	Add these VLANs to the member set.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.

Default

By default, switchport hybrid is enabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following shows adding a single VLAN to the member set.

```
(config-if)#switchport hybrid allowed vlan add VLAN_RANGE2
eg switchport hybrid allowed vlan add 2
```

The following shows adding a range of VLANs to the member set.

```
(config-if)#switchport hybrid allowed vlan add VLAN_RANGE2
eg switchport hybrid allowed vlan add 2-4
```

switchport mode

Use this command to set the switching characteristics of the Layer 2 interface.

Note: Customer-Network Port is not supported in Qumran1 series platforms.

Command Syntax

```
switchport mode (access|hybrid|trunk|provider-network|customer-edge
|customer-network|private-vlan)
```

Parameters

`access`	Access.
`hybrid`	Hybrid.
`trunk`	Trunk.
`provider-network`	Provider network.
`customer-network`	Customer network.

Default

By default, switchport mode access is enabled.

Configuring an interface to operate in trunk mode using the CLI command `switchport mode trunk` will automatically permit VLAN ID 1 on the trunk ports by default.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode access
```

switchport mode hybrid acceptable-frame-type

Use this command to set the interface acceptable frame types. This processing occurs after VLAN classification.

Command Syntax

```
switchport mode hybrid acceptable-frame-type (all|vlan-tagged)
```

Parameters

`all`	Set all frames can be received
`vlan-tagged`	Accept only classified frames that belong to the port's member set.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/ trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode hybrid acceptable-frame-type vlan-tagged
```

switchport trunk allowed

Use this command to set the switching characteristics of the interface to trunk.

For a VLAN range, specify two VLAN identifiers: the lowest and then the highest separated by a hyphen. For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces between the hyphens or commas.

Use the `no` parameter to remove all VLAN identifiers configured on this port.

Command Syntax

```
switchport trunk allowed vlan all
switchport trunk allowed vlan none
switchport trunk allowed vlan add VLAN_ID
switchport trunk allowed vlan except VLAN_ID
switchport trunk allowed vlan remove VLAN_ID
no switchport trunk
```

Parameters

`all`	Allow all VLANs to transmit and receive through the interface.
`none`	Allow no VLANs to transmit and receive through the interface.
`add`	Add these VLANs to the member set.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.
`except`	All VLANs except these VLANs are part of the member set.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.
`remove`	Remove these VLANs from the member set.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following shows adding a single VLAN to the port's member set.

```
(config)#interface eth0
(config-if)#switchport trunk allowed vlan add 2
```

The following shows adding a range of VLANs to the port's member set.

```
(config)#interface eth0
(config-if)#switchport trunk allowed vlan add 2-4
```

switchport mode trunk disable-native-vlan

Use this command to create a switchport mode trunk without any default native vlan (i.e. vlan 1).

Use the `no` form of this command to delete the CLI and add vlan-1 back as default-native-vlan (i.e. vlan 1) as untagged.

Command Syntax

```
switchport mode trunk disable-native-vlan
no switchport mode trunk disable-native-vlan
```

Parameters

None

Command Mode

Interface mode

Applicability

This command is introduced in OcNOS version 5.1.

Example

```
(config)#int xe7
(config-if)#switchport mode trunk disable-native-vlan
```

switchport trunk native

Use this command to configure native VLANs for this port. The native VLAN is used for classifying the incoming untagged packets.

Use the `no` parameter to revert the native VLAN to the default VLAN identifier 1.

Command Syntax

```
switchport trunk native vlan VLAN_ID
no switchport trunk native vlan
```

Parameter

`VLAN_ID`	VLAN identifier(s) <1-4094>. You can specify a single VLAN, or a VLAN list. For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces in between the hyphens or commas.

Default

The default is that ingress filtering is off and all frame types are classified and accepted.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport trunk native vlan 2

(config)#interface eth0
(config-if)#no switchport trunk native vlan
```

switchport mode private-vlan

Use this command to make a Layer 2 port a host port, promiscuous port, or trunk port.

Use the `no` form of this command to remove the configuration.

Command Syntax

```
switchport mode private-vlan (host | promiscuous)
no switchport mode private-vlan
```

Parameters

`host`	This port type can communicate with all other host ports assigned to the same community VLAN, but it cannot communicate with the ports in the same isolated VLAN. All communications outside of this VLAN must pass through a promiscuous port in the associated primary VLAN.
`promiscuous`	A promiscuous port can communicate with all interfaces, including the community and isolated ports within a private VLAN

Default

By default, switchport mode private-vlan is host.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 3.0.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode private-vlan host
(config)#interface eth1
(config-if)#switchport mode private-vlan promiscuous
(config)#interface eth2
(config-if)#no switchport mode private-vlan
```

switchport private-vlan association-trunk

Use this command to associate primary vlan and secondary vlan under "switchport mode trunk" and "switchport mode private-vlan host".

Note: Each secondary VLAN on a host trunk port must be associated with a different primary VLAN. User cannot put two secondary VLANs that are associated with the same primary VLAN on a host trunk port. Each secondary vlan on the same port has to have the same type, ie isolated or community, there cannot be mixed type.

Use the no form of this command to remove the association.

Command Syntax

```
switchport private-vlan association-trunk VLAN_ID VLAN_ ID
no switchport private-vlan association-trunk VLAN_ ID VLAN_ ID
no switchport private-vlan association-trunk
```

Parameters

VLAN_ ID	VLAN ID 2-4094

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.1.

Example

```
#configure terminal
(config)#interface xe2
(config-if)#speed 10g
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode trunk
(config-if)#switchport trunk allowed vlan add 10 20
(config-if)#switchport mode private-vlan host
(config-if)#switchport private-vlan association-trunk 100 10
(config-if)#switchport private-vlan association-trunk 200 20
(config-if)#no switchport private-vlan association-trunk 100 10
(config-if)#no switchport private-vlan association-trunk
```

switchport private-vlan host-association

Use this command to associate a primary VLAN and a secondary VLAN to a host port. Only one primary and secondary VLAN can be associated to a host port.

Use the `no` form of this command to remove the association.

Command Syntax

```
switchport private-vlan host-association <2-4094> add <2-4094>
no switchport private-vlan host-association
```

Parameters

`<2-4094>`	VLAN identifier of the primary VLAN.
`add`	Adds the secondary VLAN.
`<2-4094>`	VLAN identifier of the secondary VLAN (either isolated or community).

Default

By default, switchport mode private-vlan value is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport private-vlan host-association 2 add 3

#configure terminal
(config)#interface eth0
(config-if)#no switchport private-vlan host-association
```

switchport private-vlan mapping

Use this command to associate a primary VLAN and a set of secondary VLANs to a promiscuous port.

Use the `no` form of this to remove all the association of secondary VLANs to primary VLANs for a promiscuous port.

Command Syntax

```
switchport private-vlan mapping <2-4094> add VLAN_ID
switchport private-vlan mapping <2-4094> remove VLAN_ID
no switchport private-vlan mapping
```

Parameters

`<2-4094>`	VLAN identifier of the primary VLAN.
`add`	Adds the secondary VLAN.
`remove`	Removes the secondary VLAN.
`VLAN_ID`	VLAN identifier <2-4094> of the secondary VLAN (either isolated or community).

Default

By default, switchport mode private-vlan mapping value is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport private-vlan mapping 2 add 3-4
(config-if)#switchport private-vlan mapping 2 remove 3-4

(config-if)#no switchport private-vlan mapping
```

feature vlan classifier

Use this command to enable the feature VLAN classifier.

Use `no` form of this command to disable the feature VLAN classifier.

Command Syntax

```
feature vlan classifier
no feature vlan classifier
```

Parameters

`classifier`	VLAN Classifier Service

Default

By default, feature vlan classifier is enable

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#feature vlan classifier
(config)#no feature vlan classifier
```

vlan classifier activate

Use this command to activate the VLAN classifier.

Use no form of this command to deactivate the VLAN classifier.

Command Syntax

```
vlan classifier activate <1-16> vlan <2-4096>
no vlan classifier activate <1-16>
```

Parameters

<1-16>	Indicates the VLAN classifier activate identifier.
<2-4094>	VLAN identifier of the primary VLAN.

Default

By default, vlan classifier activate value is 1

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth2
(config-if)#vlan classifier activate 1 vlan 2

(config-if)#no vlan classifier activate 1
```

vlan classifier group

Use this command to create a subnet-based VLAN classifier group. A group indicates a VLAN classifier group ID.

Command Syntax

```
vlan classifier group <1-16> (add | delete) rule <1-256>
no vlan classifier group <1-16>
```

Parameters

`add`	Adds a rule to a group.
`delete`	Deletes a rule from a group.
`rule`	Indicates the VLAN classifier rule identifier `<1-256>`.

Default

By default, vlan classifier group value is 1

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan classifier group 1 delete rule 1
(config)#no vlan classifier group 1
```

vlan classifier rule ipv4

Use this command to create a subnet-based VLAN classifier rule and map it to a specific VLAN.

Use this command to create a MAC-based VLAN classifier rule and map it to a specific VLAN. If the source IP address matches the IP subnet specified in the VLAN classifier rule, received packets are mapped to the designated VLAN.

Command Syntax

```
vlan classifier rule <1-256> ipv4 A.B.C.D/M
no vlan classifier rule <1-256>
```

Parameters

`A.B.C.D/M`	Indicates the IPv4 address classification. Enter the address in A.B.C.D/M format.

Default

By default, vlan classifier rule is VLAN1

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan classifier rule 2 ipv4 20.20.20.2/24
(config)#no vlan classifier rule 2
```

vlan classifier rule mac

Use this command to create a MAC-based VLAN classifier rule and map it to a specific VLAN.

If the source MAC address matches the MAC specified in the VLAN classifier rule, received packets are mapped to the designated VLAN.

Command Syntax

```
vlan classifier rule <1-256> mac WORD
no vlan classifier rule <1-256>
```

Parameters

WORD	MAC Address in HHHH.HHHH.HHHH format.

Default

By default, vlan classifier rule value is VLAN1

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)##vlan classifier rule 2 mac 00D0.2331.AA1C
(config)#no vlan classifier rule 2
```

vlan classifier rule proto

Use this command to create an Ethertype-based VLAN classifier rule for a protocol and map it to a specific VLAN. If thesource Ethertype matches the Ethertype specified in the VLAN classifier rule, received packets are mapped to the designated VLAN.

Command Syntax

```
vlan classifier rule <1-256> proto
  (ETHERTYPE|ip|x25|arp|g8bpqx25|ieeepup|ieeeaddrtrans|dec|decdnadumpload|decdnare
  moteconsole|decdnarouting|declat|decdiagnostics|rarp|atalkddp|atalkaarp|ipx|ipv6
  |atmmulti|pppdiscovery|pppsession|atmtransport)
no vlan classifier rule <1-256>
```

Parameters

ETHERTYPE	Specify an Ethernet protocol number (0x600-0xFFFF)
arp	Address Resolution Protocol (0x0806)
atalkaarp	Appletalk AARP (0x80F3)
atalkddp	Appletalk DDP (0x809B)
atmmulti	MultiProtocol Over ATM (0x884c)
atmtransport	Frame-based ATM Transport (0x8884)
dec	DEC Assigned (0x6000)
decdiagnostics	DEC Diagnostics (0x6005)
decdnadumpload	DEC DNA Dump/Load (0x6001)
decdnaremoteconsole	DEC DNA Remote Console (0x6002)
decdnarouting	DEC DNA Routing (0x6003)
declat	DEC LAT (0x6004)
g8bpqx25	G8BPQ AX.25 (0x08FF)
ieeeaddrtrans	Xerox IEEE802.3 PUP Address Translation (0x0a01)
ieeepup	Xerox IEEE802.3 PUP (0x0a00)
ip	IP (0x0800)
ipv6	IPv6 (0x86DD)
ipx	IPX (0x8137)
pppdiscovery	PPPoE discovery (0x8863)
pppsession	PPPoE session (0x8864)
rarp	Reverse Address Resolution Protocol (0x8035)
x25	CCITT X.25 (0x0805)

Default

By default, vlan classifier rule value is VLAN1

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#vlan classifier rule 2 proto ip
(config)#no vlan classifier rule 2
(config)#vlan classifier rule 3 proto 0x0805
(config)#no vlan classifier rule 3
```

vlan database

Use this command to enter the VLAN configuration mode to add, delete, or modify values associated with a single VLAN.

Command Syntax

```
vlan database
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In the following example, note the change to VLAN configuration mode from Configure mode:

```
#configure terminal
(config)#vlan database
(config-vlan)#
```

vlan VLAN_RANGE bridge

This command allows you to create a single/range of VLAN’s on the VLAN aware bridges.

Use the no form of this command to delete the VLAN.

Command Syntax

```
vlan VLAN_RANGE bridge <1-32>
vlan <2-4094> bridge <1-32> (state (enable|disable)|)
vlan VLAN_RANGE bridge <1-32> (name WORD|) state (enable | disable)
no vlan VLAN_RANGE bridge <1-32>
```

Parameters

`VLAN_RANGE`	The vlan-id or range of vlan-id's separated by ','&'-'
`bridge`	Specify the bridge group ID in the range <1-32>.
`state`	Indicates the operational state of the VLAN.
`enable`	Sets VLAN into an enable state.
`disable`	Sets VLAN into a disable state.

Default

By default, vlan bridge state is disabled

Command Mode

Configuration Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#vlan 3-40,56 bridge 4
(config)#no vlan 2-5 bridge 2
```

vlan VLAN_RANGE type customer

This command allows you to create a single/range of VLAN's of the type Customer VLAN in Provider Edge bridges.

Use the `no` form of this command to delete the VLAN.

Command Syntax

```
vlan VLAN_RANGE (type (customer)|) bridge <1-32> (name WORD|) (state
  (disable|enable)|)
no vlan VLAN_RANGE type (customer) bridge <1-32>
no vlan VLAN_RANGE bridge <1-32>
```

Parameters

`VLAN_RANGE`	VLAN ID 2-4094 or range(s): 2-5,10 or 2-5,7-19
`bridge`	Specify the bridge group ID in the range <1-32>.
`WORD`	The ascii name of the VLAN
`state`	Indicates the operational state of the VLAN.
`enable`	Sets VLAN into an enable state.
`disable`	Sets VLAN into a disable state.
`customer`	Customer VLAN

Default

By default, vlan customer state is disabled

Command Mode

Configuration Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config-vlan)#vlan 15 type customer bridge 1 name abcde state enable
(config-vlan)#vlan 2-10,15 type customer bridge 1 state enable
(config-vlan)#no vlan 2-10,15 type customer bridge 1
(config-vlan)#
(config)#no vlan 2-10,15 br 1
(config)#end
#
```

vlan VLAN_RANGE type service

This command allows you to create a single/range of VLAN's of the type Service VLAN in Provider Edge & provider network bridges.

Use the no form of this command to delete the VLAN.

Command Syntax

```
vlan VLAN_RANGE type service (point-point|multipoint-multipoint|rooted-multipoint)
  bridge <1-32> (state (disable|enable)|)
vlan VLAN_RANGE type service (point-point|multipoint-multipoint|rooted-multipoint)
  bridge <1-32> name WORD (state (disable|enable)|)
no vlan VLAN_RANGE type service bridge <1-32>
```

Parameters

`VLAN_RANGE`	VLAN ID 2-4094 or range(s): 2-5,10 or 2-5,7-19
`service`	service VLAN
`multipoint-multipoint`	Service Multipoint to Multipoint Service VLAN
`point-point`	Service Point-to-Point Service VLAN
`rooted-multipoint`	Service Rooted Multipoint Service VLAN
`bridge`	Specify the bridge group ID in the range <1-32>.
`WORD`	The ascii name of the VLAN
`state`	Operational state of the VLAN
`disable`	Disable VLAN status on the bridge
`enable`	Enable VLAN status on the bridge

Default

By default, with the name WORD this can only be given in "vlan database" mode.

Command Mode

Configuration Mode

VLAN Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#vlan database
(config-vlan)#vlan 100 type service multipoint-multipoint bridge 1 name xxxx
state enable
(config-vlan)#vlan 101 type service point-point bridge 1 name afsa state
disable
```

```
(config-vlan)#vlan 102 type service rooted-multipoint bridge 1 state enable
(config)#vlan 104-107 type service multipoint-multipoint bridge 1 state enable
(config)#vlan 114-117,119 type service multipoint-multipoint bridge 1 state
enable
(config)#vlan 124-127,129 type service point-point bridge 1 state enable
(config)#no vlan 114-117,119 type service br 1
```

CHAPTER 9 802.1x Commands

This chapter describes the 802.1X commands.

auth-mac

Use this command to enable MAC based authentication standalone on the interface level.

Use the `no` form of this command to disable/remove the auth-MAC from interface level.

Command Syntax

```
auth-mac
no auth-mac
```

Parameters

None.

Default

Command message will not be displayed and disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#auth-mac
(config-if)#commit

#configure terminal
(config)#interface eth0
(config-if)#no auth-mac
(config-if)#commit
(config-if)#end
```

auth-mac mode

Use this command to enable MAC authentication mode on an interface.

Use the `no` parameter with this command to disable MAC authentication mode on an interface.

Command Syntax

```
auth-mac mode (filter|shutdown)
no auth-mac mode
```

Parameters

`filter`	Filter the frames for the MAC when in an unauthorized state.
`shutdown`	Shut down the interface when the MAC is unauthenticated.

Default

No default value is specified.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#auth-mac mode filter
(config-if)#commit

#configure terminal
(config)#interface eth0
(config-if)#no auth-mac mode
(config-if)#commit
```

auth-mac system-auth-ctrl

Use this command to enable MAC authentication globally. If MAC authentication is not enabled, other MAC authentication related commands throw an error when issued.

Use the `no` parameter with this command to disable MAC authentication globally.

Command Syntax

```
auth-mac system-auth-ctrl
no auth-mac system-auth-ctrl
```

Parameters

None

Default

Authentication system messages are not displayed.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#auth-mac system-auth-ctrl

(config)#no auth-mac system-auth-ctrl
```

auth-port

Use this command to specify a port for Radius authentication.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
auth-port <1-65535>
no auth-port
```

Parameters

`<0-65535>`	Port number.

Default

The default port number is 1812.

Command Mode

Configure Radius server mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Examples

```
#configure terminal
(config)#radius-server dot1x host 1.1.1.1
(config-radius-server)#auth-port 1233
(config-radius-server)#no auth-port
```

debug dot1x

Use this command to turn on or turn off 802.1x debugging at various levels.

Use the `no` parameter with this command to turn off debugging.

Command Syntax

```
debug dot1x (all|)
debug dot1x event
debug dot1x nsm
debug dot1x packet
debug dot1x timer
no debug dot1x (all|)
no debug dot1x event
no debug dot1x nsm
no debug dot1x packet
no debug dot1x timer
```

Parameters

`all`	Sets debugging for all 802.1x levels.
`event`	Sets debugging for 802.1x events.
`nsm`	Sets debugging for 802.1x NSM information.
`packet`	Sets debugging for 802.1x packets.
`timer`	Sets debugging for 802.1x timer.

Default

No default value is specified.

Command Mode

Exec, Privileged Exec, and Configure modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug dot1x all
(config)#debug dot1x event
```

dot1x mac-auth-bypass

Use this command allows you to enable/disable MAC-authentication-bypass as fallback on the interface level which has dot1x configured.

Use the `no` form of this command to remove the MAC-auth-bypass.

Command Syntax

```
dot1x mac-auth-bypass (enable|disable)
no dot1x mac-auth-bypass
```

Parameters

`dot1x`	IEEE 802.1X Port-Based Access Control
`mac-auth-bypass`	
	Quiet period in the HELD state (default 60 sec)
`disable`	Disable MAC authentication bypass
`enable`	Enable MAC authentication bypass

Default

Command message will not be displayed and disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 5.0

Examples

```
#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#int xe10
(config-if)#dot1x mac-auth-bypass enable
(config-if)#commit
(config-if)#
(config-if)#no dot1x mac-auth-bypass
(config-if)#commit
(config-if)#end
```

dot1x port-control

Use this command to force a port state.

Use the `no` parameter with this command to remove a port from the 802.1x management.

Command Syntax

```
dot1x port-control (force-unauthorized|force-authorized|auto)
no dot1x port-control
```

Parameters

`auto`	Specify to enable authentication on port.
`force-authorized`	Specify to force a port to always be in an authorized state.
`force-unauthorized`	Specify to force a port to always be in an unauthorized state.

Default

The dot1x port-control default is active.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x port-control auto

(config)#interface eth0
(config-if)#no dot1x port-control
```

dot1x protocol-version

Use this command to set the protocol version of dot1x to 1 or 2. The protocol version must be synchronized with the Xsupplicant being used in that interface.

Use the `no` parameter with this command to set the protocol version to the default value (2).

Command Syntax

```
dot1x protocol-version <1-2>
no dot1x protocol-version
```

Parameters

`<1-2>`	Indicates the EAP Over LAN (EAPOL) version.

Default

The default dot1x protocol version is 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x protocol-version 2

(config)#interface eth0
(config-if)#no dot1x protocol-version
```

dot1x quiet-period

Use this command to set the quiet-period time interval.

When a switch cannot authenticate a client, the switch remains idle for a quiet-period interval of time, then tries again. By administratively changing the quiet-period interval, by entering a lower number than the default, a faster response time can be provided.

Use the `no` parameter with this command to set the configured quiet period to the default (60 seconds).

Command Syntax

```
dot1x quiet-period <1-65535>
no dot1x quiet-period
```

Parameter

`<1-65535>`	Seconds between the retrial of authentication.

Default

The default dot1x quiet-period is 60.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x quiet-period 200
```

dot1x reauthentication

Use this command to enable reauthentication on a port.

Use the `no` parameter to disable reauthentication on a port.

Command Syntax

```
dot1x reauthentication
no dot1x reauthentication
```

Parameters

None

Default

The dot1x reauthentication default is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x reauthentication
```

dot1x reauthMax

Use this command to set the maximum reauthentication value, which sets the maximum number of reauthentication attempts after which the port will be unauthorized.

Use the `no` parameter with this command to set the reauthentication maximum to the default value (2).

Command Syntax

```
dot1x reauthMax <1-10>
no dot1x reauthMax
```

Parameter

`<1-10>`	Indicates the maximum number of reauthentication attempts after which the port will be unauthorized.

Default

The default is 2.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following sets the maximum reauthentication value to 5.

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x reauthMax 5
```

The following sets the reauthentication maximum to the default value.

```
#configure terminal
(config)#interface eth0
(config-if)#no dot1x reauthMax
```

dot1x system-auth-ctrl

Use this command to enable globally authentication.

Use the `no` parameter to disable globally authentication.

Command Syntax

```
dot1x system-auth-ctrl
no dot1x system-auth-ctrl
```

Parameters

None

Default

Authentication is off by default.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#dot1x system-auth-ctrl
```

dot1x timeout re-authperiod

Use this command to set the interval between reauthorization attempts.

Use the `no` parameter to disable the interval between reauthorization attempts.

Command Syntax

```
dot1x timeout re-authperiod <1-4294967295>
no dot1x timeout re-authperiod
```

Parameter

`<1-4294967295>` Specify the seconds between reauthorization attempts.

Default

Default time is 3600 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout re-authperiod 25
```

dot1x timeout server-timeout

Use this command to set the authentication sever response timeout.

Use the `no` parameter to disable the authentication sever response timeout.

Command Syntax

```
dot1x timeout server-timeout <1-65535>
no dot1x timeout server-timeout
```

Parameter

`<1-65535>`	Specify the authentication server response timeout.

Default

Default timeout is 30 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout server-timeout 555

(config)#interface eth0
(config-if)#no dot1x timeout server-timeout
```

dot1x timeout supp-timeout

Use this command to set the interval for a supplicant to respond.

Use the `no` parameter to disable the authentication sever response timeout.

Command Syntax

```
dot1x timeout supp-timeout <1-65535>
no dot1x timeout supp-timeout
```

Parameter

`<1-65535>`	Specify the authentication server response timeout.

Default

Default timeout is 30 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout supp-timeout 40

(config)#interface eth0
(config-if)#no dot1x timeout supp-timeout
```

dot1x timeout tx-period

Use this command to set the interval between successive attempts to request an ID.

Use the `no` parameter to disable the interval between successive attempts to request an ID.

Command Syntax

```
dot1x timeout tx-period <1-65535>
no dot1x timeout tx-period
```

Parameter

`<1-65535>`	Specify the authentication server response timeout.

Default

Default timeout is 30 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout tx-period 34

(config)#interface eth0
(config-if)#no dot1x timeout tx-period
```

ip radius source-interface

Use this command to set the local address sent in packets to the radius server.

Use the `no` parameter to clear the local address.

Command Syntax

```
ip radius source-interface A.B.C.D <1-65535>
no ip radius source-interface
```

Parameters

`A.B.C.D`	IPv4 address of the RADIUS server.
`<1-65535>`	Port number.

Default

The default port number is 1812.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip radius source-interface 12.12.12.1 1812
(config)#no ip radius source-interface
```

key-string

Use this command to define a password in plain text.

The password is stored as encrypted and is displayed in encrypted text when the `show running-config` command is executed.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
key-string WORD
no key-string
```

Parameter

`WORD`	A string of characters to use as a password (1-64 characters).

Default

By default, the password is not configured.

Command Mode

Configure Radius server mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Examples

```
#configure terminal
(config)#radius-server dot1x host 1.1.1.1
(config-radius-server)#key-string 1234567890
(config-radius-server)#no key-string
```

key-string encrypted

Use this command to define a password in encrypted format.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
key-string encrypted WORD
no key-string
```

Parameter

`WORD`	A string of characters to use as a password (18-130 characters).

Default

By default, password is not configured.

Command Mode

Configure Radius server mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Examples

```
#configure terminal
(config)#radius-server dot1x host 1.1.1.1
(config-radius-server)#key-string encrypted 0x16176d21cc1688d995
(config-radius-server)#no key-string
```

radius-server dot1x host

Use this command to specify the IP address of the remote radius server host and assign authentication and accounting destination port numbers. Multiple radius-server host commands can be used to specify multiple hosts. The software searches for hosts in the order they are specified.

If no host-specific auth-port, timeout, retransmit, key-string, or key-string encrypted values are specified, the global default values apply to that host.

Use the `no` form of the command to unconfigure a specified radius-server.

Command Syntax

```
radius-server dot1x host (A.B.C.D)
no radius-server dot1x host (A.B.C.D)
```

Parameters

`dot1x`	IEEE 802.1X Port-Based Access Control.
`A.B.C.D`	IPv4 address of the RADIUS server.

Default

The default value of auth-port is 1812.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server dot1x host 1.1.1.1
(config-radius-server)#
(config)#no radius-server dot1x host 1.1.1.1
```

retransmit

Use this command to specify the number of times to transmit each Radius request to the server before giving up.

Use the `no` form of this command to disable retransmission.

Command Syntax

```
retransmit <0-100>
no retransmit
```

Parameter

`<0-100>`	Number of times to transmit each Radius request (0-100).

Default

The default value is 3.

Command Mode

Configure Radius server mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Examples

```
#configure terminal
(config)#radius-server dot1x host 1.1.1.1
(config-radius-server)#retransmit 12
(config-radius-server)#no retransmit
```

show debugging dot1x

Use this command to display the status of the debugging of the 802.1x system.

Command Syntax

```
show debugging dot1x
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

```
#show debugging dot1x
802.1X debugging status:
```

show dot1x

Use this command to display the state of the whole system.

Command Syntax

```
show dot1x
show dot1x all
show dot1x host
show dot1x diagnostics interface IFNAME
show dot1x interface IFNAME
show dot1x sessionstatistics (interface IFNAME|)
show dot1x statistics interface IFNAME
```

Parameters

`all`	Display all information.
`host`	Show operational radius-server dot1x host information for a specific host (IPv4 address) or for all hosts.
`diagnostics`	Display diagnostics information.
`interface`	Display diagnostics interface information.
`interface`	Display interface information.
`sessionstatistics`	Display session statistics.
`interface`	Display session statistics interface information.
`statistics`	Display statistics information.
`interface`	Display statistics interface information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Displayed Output

The following tables describes the output for the show dot1x all command and the show dot1x interface command.

Table 9-25: Port variables

Entry	Description
portEnabled	Interface operational status (Up-true/down-false)
portControl	Current control status of the port for 802.1x control
portStatus	802.1x status of the port (authorized/unauthorized)

Table 9-25: Port variables

Entry	Description
reAuthenticate	Reauthentication enabled/disabled status on port
reAuthPeriod	Value holds meaning only if reAuthentication is enabled

Table 9-26: Supplicant PAE related global variables

Entry	Description
abort	Indicates that authentication should be aborted when set to true
fail	Indicates failed authentication attempt when set to false
start	Indicates authentication should be started when set to true
timeout	Indicates authentication attempt timed out when set to true
success	Indicates authentication successful when set to true

Table 9-27: 802.1x Operational State of Interface

Entry	Description
mode	Configured 802.1x mode
reAuthCount	Reauthentication count
quietperiod	Time between reauthentication attempts
reAuthMax	Maximum reauthentication attempts

Table 9-28: Backend Authentication state machine variables and constants

Entry	Description
state	State of the state machine
reqCount	Count of requests sent to server
suppTimeout	Supplicant timeout
serverTimeout	Server timeout
maxReq	Maximum requests to be sent

Table 9-29: Controlled Directions State machine

Entry	Description
adminControlledDirections	Administrative value (Both/In)

Table 9-29: Controlled Directions State machine

Entry	Description
operControlledDirections	Operational Value (Both/In)

Table 9-30: KR -- Key receive state machine

Entry	Description
rxKey	True when EAPOL-Key message is received by supplicant or authenticator. false when key is transmitted

Table 9-31: Key Transmit State machine

Entry	Description
keyAvailable	False when key has been transmitted by authenticator, true when new key is available for key exchange
keyTxEnabled	Key transmission enabled/disabled status

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is an output of this command displaying the state of the system.

```
#show dot1x
% 802.1x authentication enabled
% Radius server address: 192.168.1.1.1812
% Radius client address: dhcp128.mySite.com.12103
% Next radius message id: 0
```

The following is an output of this command displaying detailed information for all ports.

```
#show dot1x all
% 802.1x authentication enabled
% Radius server address: 192.168.1.1.1812
% Radius client address: dhcp128.mySite.com.12103
% Next radius message id: 0
% Dot1x info for interface eth1 - 3
%  portEnabled: true - portControl: auto
%  portStatus: unauthorized - currentId: 11
%  reAuthenticate: disabled
%  abort:F fail:F start:F timeout:F success:F
%  PAE: state: connecting - portMode: auto
%  PAE: reAuthCount: 2 - rxRespId: 0
%  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
%  BE: state: idle - reqCount: 0 - idFromServer: 0
%  BE: suppTimeout: 30 - serverTimeout: 30 - maxReq: 2
%  CD: adminControlledDirections: in - operControlledDirections: in
%  CD: bridgeDetected: false
```

```
%  KR: rxKey: false
%  KT: keyAvailable: false - keyTxEnabled: false
```

show mab all

Use this command to display the DOT1x timer, MAB status enabled/disabled port status (authorized/unauthorized) and last rejected MAC (if any).

Command Syntax

```
show mab all
```

Parameters

None

Default

NA

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 5.0

Examples

```
#sh mab all
Global MAC Authentication Enabled
  RADIUS client address: not configured

MAB info for interface xe10
  Dot1x timer: Expired
  MAB Authentication Enabled
  Status: Unauthorized
  Last rejected MAC:

MAB info for interface xe11
  Dot1x timer: Expired
  MAB Authentication Disabled
  Status: Unknown
  Last rejected MAC:
```

timeout

Use this command to specify the number of seconds a router waits for a reply to a Radius request before retransmitting the request.

Use the `no` parameter to use the default value.

Command Syntax

```
timeout <0-60>
no timeout
```

Parameter

`<0-60>`	Timeout period in seconds.

Default

The default value is 5 seconds.

Command Mode

Configure Radius server mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Examples

```
#configure terminal
(config)#radius-server dot1x host 1.1.1.1
(config-radius-server)#timeout 20
(config-radius-server)#no timeout
```

CHAPTER 10 Layer 2 Sub-interface Commands

This chapter is a reference for the Layer 2 sub-interface commands.

bridge-domain

Use this command to configure bridge-domain and attached sub-interfaces to it.

Use the `no` form of this command to remove the configured bridge-domain.

Command Syntax

```
bridge-domain <1-2147483647>
no bridge-domain <1-2147483647>
```

Parameters

`<1-2147483647>`	Specifies the bridge domain ID.

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
(config)#bridge-domain 1
(config-bridge-domain)#interface xe10.1
(config-bridge-domain)#interface xe11.1
(config-bridge-domain)#exit
(config)#commit
```

clear mac address-table dynamic bridge-domain

Use this command to clear dynamically learned MAC address entries from bridge-domains. This command removes specific or all dynamic MAC entries by interface, MAC address, or bridge-domain ID, to force relearning or to reset Layer 2 forwarding behavior.

Command Syntax

```
clear mac address-table dynamic bridge-domain id <1-2147483647> (interface IFNAME |
  address MAC|)
clear mac address-table dynamic bridge-domain all
```

Parameters

`interface IFNAME`	Clears dynamic MAC entries learned on a specific interface (e.g., xe1.1).
`address MAC`	Clears a specific dynamic MAC address entry. The MAC address must be in HHHH.HHHH.HHHH format (e.g., 0022.3344.5566).
`id <1-2147483647>`	Clears dynamic MAC entries associated with the specified bridge-domain ID.
`all`	Clears all dynamic MAC entries across all bridge-domains.

Command Mode

Exec mode

Applicability

Introduced in OcNOS version 6.6.1.

Examples

Clear all dynamic MAC entries in bridge-domain 1:

```
OcNOS#clear mac address-table dynamic bridge-domain id 1
```

Clear MAC entries learned on interface xe1.1 in bridge-domain 1:

```
OcNOS#clear mac address-table dynamic bridge-domain id 1 interface xe1.1
```

Clear a specific MAC address from bridge-domain 1:

```
OcNOS#clear mac address-table dynamic bridge-domain id 1 address
0022.3344.5566
```

Clear all dynamic MAC entries across all bridge-domains:

```
OcNOS#clear mac address-table dynamic bridge-domain all
```

cross-connect

Use this command to create an AC-to-AC cross-connect between the L2 sub-interfaces. It creates a separate mode with endpoint1 and endpoint2 being L2 sub-interfaces. It is possible to bind L2 sub-interface to cross-connect only when encapsulation is configured on it.

Use the `no` form of this command to remove the given cross-connect.

Command Syntax

```
cross-connect <WORD> (interface <IFNAME>) (interface <IFNAME>) (description)
  (disable)
no cross-connect <WORD>
```

Parameters

`WORD`	XC name
`IFNAME`	AC interface name
`description`	Characters describing AC cross-connect
`disable`	disables the cross-connect

Default

None

Command Mode

Configure mode for cross-connect

Cross-connect mode for IFNAME, description and disable

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
(config)#cross-connect c1
(config-xc)#interface xe1.1
(config-xc)#interface xe1.2
(config-xc)#description XC1
(config-xc)#disable
(config-xc)#exit
(config)#no cross-connect c1
(config)#
```

dot1ad ethertype

Use this command to configure the service-tpid value on parent port of a sub-interface. By this the tpid used for service tag for a sub-interface may be inherited from the one applied to parent interface.

Use `no` form of this command to revert the value to default.

Note:

- For any dot1ad sub-interface to be functional, `dot1ad ethertype` should be set to desired value as 0x88a8/ 0x9100/0x9200.
- The dot1ad ethertype command is not allowed on MLAG interfaces. Instead, configure this command on a mapped LAG interface.
- In Q2 platforms, due to hardware limitation only upto three ethertypes are supported.

Command Syntax

```
dot1ad ethertype (0x8100 | 0x88a8 | 0x9100 | 0x9200)
no dot1ad ethertype
```

Parameters

`0x8100`	IEEE 802.1Q VLAN-tagged frame
`0x88a8`	IEEE 802.1ad Provider Bridging Service VLAN tag identifier (S-Tag)
`0x9100`	Supported for interoperability with legacy devices
`0x9200`	Supported for interoperability with legacy devices

Default

Default value is `0x`8100

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
(config)#interface xe1
(config-if)#dot1ad ethertype 0x9100
(config-if)#exit
(config)#interface xe1
(config-if)#no dot1ad ethertype
(config-if)#exit
```

encapsulation

Use this command to configure encapsulation-type for a Layer 2 sub-interface. With this command, a Layer 2 sub-interface can be configured as single-tagged with single/multiple VLANs or double-tagged, or default or untagged. Operational state of the Layer 2 sub-interface is DOWN before configuring the encapsulation and it becomes UP once the encapsulation is configured.

Use the `no` form of this command to remove the encapsulation.

Note:

- For encapsulation with a VLAN range in an inner tag or outer tag, overlapping VLANs either as a single value or a range will not be allowed under same parent port.
- Y.1731 and CFM are not supported on the same physical port when sub-interfaces are configured with untagged encapsulation and default settings.

Command Syntax

```
encapsulation ((dot1q | dot1ad | default | untagged) (vlan-id | vlanid-range)
  (inner-dot1q (vlan-id | vlanid-range)))
no encapsulation ((dot1q | dot1ad | default | untagged) (vlan-id | vlanid-range)
  (inner-dot1q (vlan-id | vlanid-range)))
```

Parameters

`dot1q`	IEEE802.1Q VLAN-tagged packets
`dot1ad`	IEEE802.1ad VLAN-tagged packets
`default`	IEEE default packets
`untagged`	IEEE untagged packets
`vlan-id`	VLAN identifier <2-4094>
`vlanid-range`	VLAN ID range(s): 2-5 10 or 2-5 7-19
`inner-dot1q`	Inner-VLAN for double-tagged

Default

None

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 3.0.

Inner-VLAN range support was introduced in OcNOS version 4.1.

Multiple encapsulation on a L2 sub-interface introduced in OcNOS version 5.0.

The `no` form of this command with parameters introduced in OcNOS version 5.0.

Example

```
(config)#interface xe1.1 switchport
(config-if)#encapsulation dot1q 10
```

```
(config-if)#ex
(config)#interface xe1.2 switchport
(config-if)#encapsulation dot1ad 11
(config-if)#ex
(config)#interface xe1.3 switchport
(config-if)#encapsulation default
(config-if)#ex
(config)#interface xe1.4 switchport
(config-if)#encapsulation untagged
(config-if)#ex
(config)#interface xe1.5 switchport
(config-if)#encapsulation dot1q 15-20
(config-if)#ex
(config)#interface xe1.6 switchport
(config-if)#encapsulation dot1ad 21-25
(config-if)#ex
(config)#interface xe1.7 switchport
(config-if)#encapsulation dot1q 100 inner-dot1q 10
(config-if)#ex
(config)#interface xe1.8 switchport
(config-if)#encapsulation dot1ad 200 inner-dot1q 20
(config-if)#ex
(config)#interface xe1.9 switchport
(config-if)#encapsulation dot1ad 300 inner-dot1q 100-200
(config-if)#ex
(config)#interface xe1.10 switchport
(config-if)#encapsulation dot1q 3999
(config-if)#encapsulation dot1ad 3998
(config-if)#ex
(config)#interface xe1.10 switchport
(config-if)#no encapsulation
(config-if)#ex
(config)#interface xe1.1 switchport
(config-if)#no encapsulation dot1q 10
(config-if)#ex
(config)#interface xe1.2 switchport
(config-if)#no encapsulation dot1ad 11
(config-if)#ex
(config)#interface xe1.3 switchport
(config-if)#no encapsulation default
(config-if)#ex
(config)#interface xe1.4 switchport
(config-if)#no encapsulation untagged
(config-if)#ex
(config)#interface xe1.5 switchport
(config-if)#no encapsulation dot1q 15-20
(config-if)#ex
(config)#interface xe1.6 switchport
(config-if)#no encapsulation dot1ad 21-25
(config-if)#ex
```

```
(config)#interface xe1.7 switchport
(config-if)#no encapsulation dot1q 100 inner-dot1q 10
(config-if)#ex
(config)#interface xe1.8 switchport
(config-if)#no encapsulation dot1ad 200 inner-dot1q 20
(config-if)#ex
(config)#interface xe1.9 switchport
(config-if)#no encapsulation dot1ad 300 inner-dot1q 100-200
(config-if)#ex
```

interface switchport

Use this command to configure a L2 sub-interface. An L2 sub-interfaces makes it possible for a logical interface to be created on an Ethernet physical interface as well as on dynamic/static LAG interfaces to handle one slice of its resource. The supported method for this resource slicing is vlan credential based which can be a single tagged or double-tagged or untagged or default along with encapsulation types as either dot1q or dot1ad.

Use `no` form of this command to unconfigure a sub-interface.

Command Syntax

```
interface IFNAME.SUBINTERFACE_ID switchport
no interface IFNAME.SUBINTERFACE_ID
```

Parameters

`IFNAME`	Interface name, such as xe1, po1 or sa1
`SUBINTERFACE_ID`	sub-interface identifier <1-2000>
`switchport`	L2 sub-interface

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
(config)#interface xe1.1 switchport
(config-if)#exit
(config)#no interface xe1.1
(config)#interface po1.1 switchport
(config-if)#exit
(config)#no interface po1.1
(config)#interface sa1.1 switchport
(config-if)#exit
(config)#no interface sa1.1
(config)#exit
#
```

mac address IFNAME

Use this command to add a static MAC address entry to a Layer 2 sub-interface-based bridge-domain. The MAC address is either forwarded to a specific sub-interface or denied from it. This command controls traffic forwarding at the MAC level within a bridge-domain.

Use the `no` parameter of this command to remove the configured static MAC address.

Command Syntax

```
mac  XXXX.XXXX.XXXX  (deny | forward) IFANME
no mac XXXX.XXXX.XXXX
```

Parameters

`mac XXXX.XXXX.XXXX`	Specifies the MAC address in HHHH.HHHH.HHHH format (e.g., 0001.0001.0002).
`deny`	Drops frames with this MAC address received on the specified sub-interface.
`forward`	Forwards frames with this MAC address to the specified sub-interface.
`IFNAME`	Specifies the name of the sub-interface (e.g., xe1.2).

Command Mode

Bridge Domain mode

Applicability

Introduced in OcNOS version 6.6.1.

Examples

Configure a static MAC forwarding rule and a deny rule on a Bridge-Domain:

```
OcNOS(config)#bridge-domain 1
OcNOS(config-bridge-domain)#mac 0001.0001.0002 forward xe1.2
OcNOS(config-bridge-domain)#mac 0001.0001.0003 deny xe1.3
OcNOS(config-bridge-domain)#exit
OcNOS(config)#exit
OcNOS#show running-config bridge-domain
!
bridge-domain 1
 interface xe1.2
 interface xe1.3
 mac 0001.0001.0002 forward xe1.2
 mac 0001.0001.0003 deny xe1.3
!
!
```

To remove the static entry:

```
OcNOS(config-bridge-domain)#no mac 0001.0001.0002
```

no subinterfaces

Use this command to remove all the sub-interfaces of any type (layer 2 or layer 3) created under a parent port.

Command Syntax

```
no subinterfaces
```

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
(config)#interface xe1
(config-if)#no subinterfaces
(config-if)#exit
```

rewrite

Use this command to manipulate the VLAN tags in the incoming packet. Supported operations are PUSH, DOUBLE PUSH, POP, DOUBLE POP and TRANSLATE on the VLAN tag with any of this ethertype - 8100/ 88a8/ 9100/ 9200.

Use the `no` form of this command to unconfigure rewrite.

Note:

- **Apply VLAN Push Rewrite:** For outgoing traffic on sub-interface "interface IFNAME", the "rewrite push" command will pop the VLAN. The egress pop removes whatever outer VLAN tag is present, regardless of its value. For incoming traffic at sub-interface "interface IFNAME", the "rewrite push" command will add a VLAN tag with TPID values 8100.
- **Apply VLAN Pop Rewrite:** For outgoing traffic on sub-interface "interface IFNAME", the "rewrite pop" command will add a VLAN tag with TPID values 8100. For incoming traffic at sub-interface "interface IFNAME", the "rewrite pop" command will pop the VLAN.
- **Apply VLAN Translate Rewrite:** For outgoing and incoming traffic at sub-interface "interface IFNAME", the "rewrite translate" command will update a VLAN tag with TPID values 9100.

Command Syntax

```
rewrite translate (( 1-to-1 | 2-to-1 ) (dot1q|dot1ad|VALUE) VLAN_RANGE2 | ( 1-to-2
  | 2-to-2 ) (dot1q|dot1ad|VALUE) VLAN_RANGE2 (dot1q|VALUE) VLAN_RANGE2 )
rewrite (pop | pop-2tag | push (dot1q|dot1ad|VALUE) VLAN_RANE2 (inner-dot1q <1-
  4095>|) )
no rewrite
```

Parameters

`pop`	Pop the outer VLAN ID (VID) before service transmission.
`push`	Push a VLID before service transmission.
`translate`	Translate the outer VID
`1-to-1`	Translates the outermost tag to another tag
`1-to-2`	Translates the outermost tag to two tags (is translate & push)
`2-to-1`	Translates the outermost two tags to another tag
`2-to-2`	Translates the outermost two tags to two other tags
`dot1q`	IEEE 802.1Q VLAN-tagged packets.
`dot1ad`	IEEE 802.1ad VLAN-tagged packets
`VALUE`	Set service TPID value as 0x8100/0x88a8/0x9100/0x9200
`VLAN_RANE2`	Service VLAN ID
`inner-dot1q <1-4095>`	Push inner-VLAN ID for double-tagged.
`pop-2tag`	Pop both the outer VID and inner VID.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
(config)#interface xe1.1 switchport
(config-if)#rewrite pop
(config-if)#exit

(config)#interface xe1.2 switchport
(config-if)#rewrite push 9100 3
(config-if)#exit

(config)#interface xe1.10 switchport
(config-if)#rewrite translate 9200 4
(config-if)#exit

(config)#interface xe1.10 switchport
(config-if)#rewrite push 0x8100 200 inner-dot1q 300
(config-if)#exit

(config)#interface xe1.1 switchport
(config-if)#rewrite pop-2tag
(config-if)#exit
(config)#interface xe1.1 switchport
(config-if)#no rewrite
(config-if)#ex
```

show bridge-domain

Use this command to display bridge-domain ID.

Command Syntax

```
show bridge-domain (<1-2147483647>|)
```

Parameters

`<1-2147483647>`	Specifies the bridge domain ID.

Default

Default

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
OcNOS#show bridge-domain

Bridge Id  interfaces       Status
----------+----------------+-----------
 1           xe10.1           UP
             xe11.1           UP
OcNOS#
```

show cross-connect

Use this command to display the cross-connected sub-interfaces along with their status and total number of cross-connects configured in the system.

Command Syntax

```
show cross-connect (WORD|)
```

Parameters

WORD	(Optional) Specifies the cross-connect name.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#show cross-connect
cross-connect status
XC name                         Ep1              Ep2              Status
-------------------------------+----------------+----------------+-------
c1                              xe1.1            xe1.2            UP
-------------------------------+----------------+----------------+-------
AC cross-connect summary
Total : 1
Up    : 1
Down  : 0
#show cross-connect c1
cross-connect status
XC name                         Ep1              Ep2              Status
-------------------------------+----------------+----------------+-------
c1                              xe1.1            xe1.2            UP
-------------------------------+----------------+----------------+-------
```

show mac address-table bridge-domain

Use this command to display MAC address entries, either dynamically learned or statically configured, associated with bridge domains. This command helps verify how MAC addresses are mapped to sub-interfaces or bridge-domain IDs.

Command Syntax

```
show mac address-table (dynamic | static) bridge-domain {interface IFNAME |address
  MAC | (id <1-2147483647> | all)}
```

Parameters

`dynamic bridge-domain`	Displays MAC addresses that have been dynamically learned through data plane traffic.
`static bridge-domain`	Displays MAC addresses that have been manually configured using static MAC commands.
`interface IFNAME`	Displays MAC entries associated with a specific interface or sub-interface (e.g., xe1.1).
`address MAC`	Displays information about a specific MAC address (in HHHH.HHHH.HHHH format).
`id <1-2147483647>`	Displays MAC entries within a specific bridge-domain ID.
`all`	Displays MAC entries across all bridge-domains.

Command Mode

Exec mode

Applicability

Introduced in OcNOS version 6.6.1.

Examples

Display MAC entries in a specific bridge-domain (ID 1):

```
OcNOS#show mac address-table dynamic bridge-domain id 1
Bridge  MAC Address     Type     Ports
------- --------------- -------- --------
1       0022.3344.5566  dynamic  xe1.1

OcNOS#show mac address-table static bridge-domain id 1
Bridge  MAC Address     Type      Ports
------+---------------+---------+---------+
1 0000.0100.0001  static    sa1.1
```

Display MAC entries for all bridge-domains:

```
OcNOS#show mac address-table dynamic bridge-domain all

Bridge  MAC Address     Type      Ports
------+---------------+---------+---------+

1    0000.0100.0001  static    xe1.1
2 0010.9400.0002  static    xe2.1
```

```
OcNOS#show mac address-table static bridge-domain all
Bridge  MAC Address     Type      Ports
------+---------------+---------+---------+
100    0000.0100.0001  static    sa1.1
100    0000.0100.0002  static    sa2.1
```

Display MAC entries learned on a specific interface:

```
OcNOS#show mac address-table dynamic bridge-domain interface xe1.1
Bridge  MAC Address     Type     Ports
------- --------------- -------- --------
1       0022.3344.5566  dynamic  xe1.1

OcNOS#show mac address-table static bridge-domain interface sa1.1
Bridge  MAC Address     Type      Ports
------+---------------+---------+---------+
100    0000.0100.0001  static    sa1.1
```

Display MAC entries learned on a specific MAC address:

```
OcNOS#show mac address-table dynamic bridge-domain address 0022.3344.5566
Bridge MAC Address Type Ports
------+---------------+---------+---------+
1 0022.3344.5566 dynamic xe1.1

OcNOS#show mac address-table static bridge-domain address 0000.0100.0001
Bridge  MAC Address     Type      Ports
------+---------------+---------+---------+
100    0000.0100.0001  static    sa1.1
```

Table 10-32: show mac address-table dynamic bridge-domain output fields

Field	Description
Bridge	Bridge-Domain ID. Identifies the Layer 2 broadcast domain in which the MAC address is learned.
MAC Address	The 48-bit MAC address (in HHHH.HHHH.HHHH format) learned within the bridge-domain.
Type	Indicates how the MAC address was learned. In this output, it is typically dynamic or static.
Ports	The interface or sub-interface (e.g., xe1.1) where the MAC address was learned. If the MAC is reachable via multiple ports (in case of EVPN or port aggregation), multiple interfaces may be listed.

CHAPTER 11 Port Security Commands

This chapter describes the port security commands.

port-security

Use this command to enable or disable port security globally.

Command Syntax

```
port-security (enable | disable)
```

Parameters

`enable`	Enable port security globally
`disable`	Disable port security globally

Default

By default, port security is enabled globally.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 4.0.

Examples

```
(config)#port-security enable
(config)#
```

show port-security

Use this command to display the port security configuration for all interfaces or for a particular interface.

Command Syntax

```
show port-security (interface IFNAME |)
```

Parameters

IFNAME	Interface name

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 4.0.

Examples

```
#show port-security
Port port-security mode MAC limit CVLAN SVLAN static secure MAC
-----------------------------------------------------------------
ge1  dynamic            3         2           0000.0000.1112
                                   10          0000.0000.3333

#show port-security interface ge1
Port Security Mode : Dynamic
Secure MAC limit : 3
Static Secure MAC list :
CVLAN SVLAN MAC Address
---------------------------
2           0000.0000.1112
10          0000.0000.3333
```

switchport port-security

Use this command to enable port security on an interface.

Use the `no` form of this command to disable port security on an interface. This command removes configured secured MAC, if any, on this interface.

Note: This command is supported for physical, LAG, and MLAG (active) interfaces only. Enabling port security on an interface removes learned MAC addresses of interfaces (whether learned by static or dynamic means), and then relearns the secure MAC addresses. Multicast MAC addresses are not considered as part of the MAC learning limit.

Note: This command is ignored when port security is already enabled on an interface.

Command Syntax

```
switchport port-security (static |)
no switchport port-security
```

Parameters

`static`	Static mode

Default

By default this feature is disabled; the default mode of port security is to dynamically learn. In dynamic mode, devices learn MAC addresses dynamically. You can program static MACs, however, dynamic MAC learning will not be allowed in static mode for port security.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 4.0.

Examples

```
#configure terminal
(config)#interface ge1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode hybrid
(config-if)#switchport hybrid allowed vlan all
(config-if)#switchport port-security
```

switchport port-security logging

Use this command to enable violated MAC logging on a port security enabled interface.

Use the `disable` parameter with this command to disable violated mac logging on a port security enabled interface.

Note: This command has no impact, as Qumran does not support unsecured MAC address logging.

Command Syntax

```
switchport port-security logging (enable | disable)
```

Parameters

`enable`	Enable violated MAC logging
`disable`	Disable violated MAC logging

Default

By default logging is disabled.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 4.0.

Examples

```
#configure terminal
(config)#interface ge1
(config-if)#switchport port-security logging enable
```

switchport port-security mac-address

Use this command to add static secure MAC addresses.

Use the `no` form of this command to remove static secure MAC addresses.

Command Syntax

```
switchport port-security mac-address XXXX.XXXX.XXXX
no switchport port-security mac-address XXXX.XXXX.XXXX
switchport port-security mac-address XXXX.XXXX.XXXX vlanId <2-4094>
no switchport port-security mac-address XXXX.XXXX.XXXX vlanId <2-4094>
switchport port-security mac-address XXXX.XXXX.XXXX svlanId <2-4094>
no switchport port-security mac-address XXXX.XXXX.XXXX svlanId <2-4094>
switchport port-security mac-address XXXX.XXXX.XXXX vlanId <2-4094> svlanId <2-
  4094>
no switchport port-security mac-address XXXX.XXXX.XXXX vlanId <2-4094> svlanId <2-
  4094>
```

Parameters

`XXXX.XXXX.XXXX`	Static secure MAC address
`vlanId`	VLAN identifier
`<2-4094>`	VLAN identifier
`svlanId`	SVLAN identifier
`<2-4094>`	SVLAN identifier

Default

N/A

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 4.0.

Examples

```
#configure terminal
(config)#interface ge1
(config-if)#switchport port-security mac-address 0000.0000.1112 vlan 2
(config-if)# no switchport port-security mac-address 0000.0000.1112 vlan 2
(config)#interface ge2
(config-if)#switchport port-security mac-address 0000.1111.2222
(config-if)#no switchport port-security mac-address 0000.1111.2222
(config)#interface ge3
(config-if)#switchport port-security mac-address 0000.2222.3333 svlan 9
(config-if)#no switchport port-security mac-address 0000.2222.3333 svlan 9
(config)#interface ge4
```

```
(config-if)#switchport port-security mac-address 0000.2222.3333 vlan 23 svlan
31
(config-if)#no switchport port-security mac-address 0000.2222.3333 vlan 23
svlan 31
```

switchport port-security maximum

Use this command to set the MAC address learning limit for an interface.

Note: This command is supported for physical, LAG, and MLAG (active) interfaces only. When a newly configured maximum learn limit is less than the previous value, you must remove/flush-out the unwanted MACs to stop traffic forwarding from the unwanted source MAC addresses. MAC addresses can be removed using the clear mac address-table command.

Use `no` form cli to set the maximum limit back to default value 1.

Command Syntax

```
switchport port-security maximum <1-1000>
no switchport port-security maximum
```

Parameters

`<1-1000>`	Maximum MAC address learning limit

Default

The default MAC address learning limit is 1.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 4.0.

Examples

```
#configure terminal
(config)#interface ge1
(config-if)#switchport port-security maximum 3

#configure terminal
(config)#interface po1
(config-if)#switchport port-security maximum 3

#configure terminal
(config)#interface mlag1
(config-if)#switchport port-security maximum 3
```

CHAPTER 12 Layer 2 Control Protocols Tunneling Commands

This chapter is a reference for the Layer 2 Control Protocols (L2CP) tunneling commands:

clear l2protocol interface counters

This command allows you to clear the counters for numbers of packets peered, discarded and tunneled.

Command Syntax

```
clear l2protocol interface (IFNAME|) counters (peer|discard|tunnel|tunnel-discard|)
```

Parameters

`peer`	Clear stats for Peer protocol packets.
`discard`	Clear stats for Tunnel protocol packets.
`tunnel`	Clear stats for Tunnel protocol packets.
`tunnel-discard`	Clear stats for Tunnel discard protocol packets.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 3.0.

Examples

```
# clear l2protocol interface xe1 counters peer
```

l2protocol

This command allows you to change the process of protocol to peer/discard/tunnel.

Command Syntax

```
l2protocol (stp|lacp|efm|elmi|lldp|synce)(peer|discard|tunnel)
```

Parameters

`stp`	Spanning Tree Protocols.
`lacp`	Link Aggregation (LACP).
`efm`	Ethernet first mile (Link OAM).
`elmi`	Ethernet local management interface.
`lldp`	Link layer discovery protocol.
`synce`	Link layer discovery protocol.
`peer`	Act as peer to the customer Device instance of the protocol.
`discard`	Discard the protocol data unit.
`tunnel`	Tunnel the Protocol data unit into the SVLAN.

Default

Default process value is peer.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 3.0.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode customer-edge access
(config-if)#l2protocol stp tunnel
(config-if)#l2protocol stp peer
(config-if)#l2protocol stp discard
```

l2protocol encapsulation dest-mac

Use this command to change destination mac of tunneled l2 protocol packet. Allowed mac are 0100.C2CD.CDD0 or 0104.DFCD.CDD0.

Use the `no` parameter with this command to set default mac 0100.C2CD.CDD0.

Note: This command only applies to provider bridging. For more information, see the *OcNOS Carrier Ethernet Guide*.

Command Syntax

```
bridge <1-32> l2protocol encapsulation dest-mac XXXX.XXXX.XXXX
no bridge <1-32> l2protocol encapsulation dest-mac
```

Parameters

`bridge`	Bridge group for bridging.
`<1-32>`	<1-32>
`l2protocol`	Configure Layer2 Protocol Tunneling.
`encapsulation`	Encapsulation of L2PT packet.
`dest-mac`	Encapsulation with destination mac.
`XXXX.XXXX.XXXX`	Destination Mac-address of L2PT tunneling (0100.C2CD.CDD0 or 0104.DFCD.CDD0).

Command Mode

Configuration mode

Applicability

This command is introduced in OcNOS version 3.0.

Examples

```
(config)#bridge 1 l2protocol encapsulation dest-mac ?
XXXX.XXXX.XXXX Destination Mac-address of L2PT tunneling (0100.C2CD.CDD0 or
0104.DFCD.CDD0)
(config)#bridge 1 l2protocol encapsulation dest-mac 0104.DFCD.CDD1
L2PT destination mac should be 0100.C2CD.CDD0 or 0104.DFCD.CDD0
(config)#bridge 1 l2protocol encapsulation dest-mac 0104.DFCD.CDD0
(config)#bridge 1 l2protocol encapsulation dest-mac 0100.C2CD.CDD0
(config)#bridge 1 l2protocol encapsulation dest-mac 0100.C2CD.CDD1
L2PT destination mac should be 0100.C2CD.CDD0 or 0104.DFCD.CDD0
(config)#

(config)#no bridge 1 l2protocol encapsulation dest-mac
(config)#show running-config | in bridge
bridge 1 protocol provider-rstp edge
vlan 2-10 type customer bridge 1 state enable
vlan 11-12 type service point-point bridge 1 state enable
cvlan registration table map1 bridge 1
bridge-group 1
bridge-group 1
(config)#
```

show l2protocol interface counters

This command allows you to display the counters for numbers of packets peered, discarded and tunneled.

Note: In case of Provider-Bridging, tunneling will be done via slow path forwarding (via CPU).

And for other tunneling feature such as L2VPN, EVPN cases, L2protocol will follow hardware forwarding path to be tunneled.

Except Provider-Bridging feature, for other tunneling feature such as L2VPN/EVPN cases, tunnel counters will not be captured. Peering and discarding decision will be taken at CPU, hence, these counters will be captured with this show command.

Command Syntax

```
show l2protocol interface (IFNAME|) counters (peer|discard|tunnel|tunnel-discard|)
```

Parameters

`peer`	Display stats for Peer protocol packets.
`discard`	Display stats for Tunnel protocol packets.
`tunnel`	Display stats for Tunnel protocol packets.
`tunnel-discard`	Display stats for Tunnel discard protocol packets.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 3.0.

Examples

```
# show l2protocol interface xe1 counters peer
Interface xe1
Peer:     stp:    1

# show l2protocol interface xe1 counters
Interface xe1
Peer:     stp:    1
Discard:  stp:    10
Tunnel:   stp:    5
```

show l2protocol processing interface

This command allows you to display the processing information on Layer 2 protocol interface.

Command Syntax

```
show l2protocol processing interface IFNAME
```

Parameters

IFNAME	Interface name

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command is introduced was before OcNOS version 3.0.

Examples

```
#show l2protocol processing interface xe1/1
Bridge    Interface Name                Protocol       Processing Status
======    ==============                ========       =================
1         xe1/1                          stp            Tunnel
1         xe1/1                          gmrp           Peer
1         xe1/1                          gvrp           Peer
1         xe1/1                          mmrp           Peer
1         xe1/1                          mvrp           Peer
1         xe1/1                          lacp           Peer
1         xe1/1                          lldp           Peer
1         xe1/1                          efm            Peer
1         xe1/1                          elmi           Peer
1         xe1/1                          ptp            Peer
1         xe1/1                          synce          Peer
```

CHAPTER 13 Errdisable Commands

This chapter describes the errdisable commands.

errdisable cause

Use this command to globally shut down a port when certain errors happen:

- BPDU guard puts an interface configured for Spanning Tree Protocol (STP) Port Fast into the ErrDisable state upon receipt of a STP BPDU to avoid a potential bridging loop.
- If one side of a link-access group (LAG) is configured as a static LAG and the other side as a dynamic LAG, the ports on the side receiving LACP BPDUs go into the ErrDisable state

Note: When link-flap ErrDisable is enabled globally, then all interfaces are enabled. Link-flap ErrDisable can be enabled globally, but disabled for a specific interface with the `no link-flap errdisable` command.

Note: Stp-Bpdu-Guard is enabled by default on the global level configuration.

Use `no` form of this command to not shut down a port when certain errors happen.

Command Syntax

```
errdisable cause {stp-bpdu-guard|lag-mismatch|link-flap|mac-move-limit}
no errdisable cause {stp-bpdu-guard|lag-mismatch|link-flap|mac-move-limit}
```

Parameters

`stp-bpdu-guard`	ErrDisable on stp-bpdu-guard
`lag-mismatch`	ErrDisable on lag-mismatch
`link-flap`	ErrDisable on link-flap
`mac-move-limit`	Enable or Disable Mac-Move-Limit

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#errdisable cause lag-mismatch
```

errdisable link-flap-setting

Use this command to configure the link-flap errdisable feature:

- An interface should change state as up-down to complete one cycle of a link flap.
- The LED does not glow when an interface is in the errdisable state.
- Errdisable is supported only on physical interfaces.
- A LAG interface does not go into the errdisable state when all of its member ports are in the errdisable state
- The error disable computation is based on a sliding window of time. The window size is configurable in seconds. This window is taken as the current time to the last <t> second, where <t> is the configured window size. If the accumulated link flap count reaches the maximum flap count for a particular sliding window, a link flap error disable fault is triggered.

Note: Any previous flapping accumulated is flushed when you execute this command.

Command Syntax

```
errdisable link-flap-setting max-flaps <1-100> time <1-1800>
```

Parameters

<1-100>	Maximum flap count
<1-1800>	Sliding window size in seconds

Default

Five flaps in ten seconds:

Maximum flap count: 5

Sliding window size: 10 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#errdisable link-flap-setting max-flaps 5 time 20
```

errdisable storm-control

Use this command to configure the storm-control errdisable. Following are the limitation:

- An interface discards BUM traffic during the specified interval to complete one discard-hit cycle.
- The LED does not glow when an interface is in the errdisable state.
- Errdisable is supported only on physical interfaces.
- A LAG interface does not go into the errdisable state when all of its member ports are in the errdisable state.
- The error disable computation is based on a sliding window of time. The window size is configurable in seconds. This window is taken as the current time to the last <t> second, where <t> is the configured window size. Every 5 seconds, a discard hit count increases if there is BUM traffic being dicarded in that period. If the accumulated discard hit count reaches the maximum count for a particular configurable sliding window, a storm control error disable fault is triggered.

Note: Any previous discard hits accumulated are flushed when you execute this command.

Command Syntax

```
errdisable storm-control discard-hit <1-100> time <1-1800>
no errdisable cause storm-control
```

Parameters

`discard-hit <1-100>`
: The maximum number of times that BUM traffic can hit the configured bandwidth threshold in an interface within a certain time window before disabling the interface. During continuous storm control discards, this counter is increased approximately every 5 seconds. Default value is 1.

`time <1-1800>`
: Sliding window size in seconds. The time window in seconds in which to consider storm control threshold hits for the purposes of disabling the interface if the discard-hit is overcome during that time. This value must have a minimum value of 6 times discard-hit. Default value is 5 seconds.

Default

- One hit: ten seconds
- Maximum discard hit count: 1
- Sliding window size: 5 seconds

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.5.1

Examples

```
#configure terminal
(config)#errdisable storm-control discard-hit 3 time 20
```

errdisable mac-move-limit

Use this command to set the ErrDisable mac movement limit.

Command Syntax

```
errdisable mac-move-limit <1-1000>
no errdisable mac-move-limit
```

Parameters

<1-1000>	Allowed Mac movement in 5 seconds

Default

By default, mac-move-limit is 1000

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 3.0.

Examples

```
#configure terminal
(config)#errdisable mac-move-limit 50
(config)#no errdisable mac-move-limit
```

errdisable timeout

Use this command to set the ErrDisable auto-recovery timeout interval.

Command Syntax

```
errdisable timeout interval <10-1000000>
```

Parameters

<10-1000000>	Timeout interval in seconds

Default

By default, zero: timer is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#errdisable timeout interval 1000
```

link-flap errdisable

Use this command to shut down the interface when it continually goes up and down.

The link-flap ErrDisable feature must be enabled globally with the errdisable cause command.

Note: When link-flap ErrDisable is enabled globally, then all interfaces are enabled. Link-flap ErrDisable can be enabled globally, but disabled for a specific interface with the `no link-flap errdisable` command.

Note: This feature is supported only on physical ports.

Use the `no` form of this command to disable this behavior.

Command Syntax

```
link-flap errdisable
no link-flap errdisable
```

Parameter

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1/1
(config-if)#link-flap errdisable
```

mac-move-limit priority

Use this command to set a priority value to an interface during MAC movement events. The system uses this priority to decide which interface to bring down when MAC movement exceeds the configured limit.

Note:

- The interface with the lower priority goes down first.
- If multiple interfaces have the same priority, the interface with the lower index goes down.

Command Syntax

```
mac-move-limit priority <0-255>
```

Parameters

<0-255>	Specifies the MAC movement limit priority range. A higher value indicates a higher priority. Interfaces with a higher priority value remain active longer during MAC move events.

Default

The default priority of each interface is zero.

Command Mode

Interface mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

```
OcNOS(config)#interface ce2
OcNOS(config-if)#mac-move-limit priority 250
OcNOS(config-if)#commit

OcNOS#show running-config interface ce2
!
interface ce2
 mac-move-limit priority 250
!
OcNOS#
```

show errdisable details

Use this command to display ErrDisable settings.

Command Syntax

```
show errdisable details
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show errdisable details
```

show interface errdisable status

Use this command to display ErrDisable conditions for an interface.

Command Syntax

```
show interface errdisable status
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface errdisable status
ge1 lag-mismatch-errdisable
ge2 stp-bpdu-guard-errdisable
```

CHAPTER 14 Unidirectional Link Detection Commands

This section describes the Unidirectional Link Detection (UDLD) commands.

udld

Use this command to enable the UDLD feature globally.

Use no form of this command to disable the UDLD feature globally.

Command Syntax

```
udld  enable
no udld enable
```

Parameters

None

Default

Disabled

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
(config)#udld enable

(config)#no udld enable
```

udld message-time

Use this command to set the UDLD message interval.

Command Syntax

```
udld message-time <7-90>
```

Parameters

<7-90>	Interval time in seconds

Default

15 seconds

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
config)#udld message-time 50
```

udld mode

Use this command to configure UDLD mode as aggressive or normal.

Command Syntax

```
udld mode (aggressive | normal)
```

Parameters

`aggressive`	Aggressive mode
`normal`	Normal mode

Default

N/A

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
(config-if)#udld mode aggressive
```

udld state

Use this command to enable or disable the UDLD feature for an interface.

Command Syntax

```
udld state (enable | disable)
```

Parameters

None

Default

Disabled

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
(config)#int xe7
(config-if)#udld state enable
```

show udld

Use this command to display UDLD statistic for all interface.

Command Syntax

```
show udld
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#show udld
UDLD                    : Enable
Message Interval(sec)   : 15
Port   UDLD Status    Mode           Link-Status
------------------------------------------------
xe7    Enable         Normal         Bi-Directional
```

Table 14-33 explains the output fields.

Table 14-33: show udld output fields

Field	Description
UDLD	Whether UDLD is enabled or disabled
Message Interval	Message interval in seconds
Port	Interface name
UDLD Status	Whether UDLD is enabled or disabled on the interface
Mode	Whether the mode is aggressive or normal
Link-Status	State of the link: Unknown Loop-Back Neighbor Mismatch Unidirectional Undetermined Bi-Directional

show udld interface

Use this command to display UDLD settings for particular interface.

Command Syntax

```
show udld interface IFNAME
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#show udld interface xe14
UDLD Status           : Enable
UDLD Mode             : Aggressive
Link-State            : Bi-Directional
#
```

Table 14-34 explains the output fields.

Table 14-34: show udld interface output fields

Field	Description
UDLD Status	Whether UDLD is enabled or disabled
UDLD Mode	Whether the mode is aggressive or normal
Link-State	State of the link: Unknown Loop-Back Neighbor Mismatch Unidirectional Undetermined Bi-Directional

CHAPTER 15 Link Layer Discovery Protocol Commands

This chapter describes the Link Layer Discovery Protocol (LLDP) commands.

lldp debug

Use this command to set the debugging functions for LLDP.

Use the no form of this command to turn off LLDP debugging functions

Command Syntax

```
lldp debug (event|rx|tx|message)
no lldp debug (event|rx|tx|message)
```

Parameters

`event`	Enable or disable event debugging
`message`	Enable or disable NSM message debugging
`rx`	Enable or disable RX debugging
`tx`	Enable or disable TX debugging

Command Mode

Exec mode and Privileged Exec mode

Examples

```
#lldp debug event
#lldp debug messages
```

lldp (disable|enable) default-agent

Use this command to exclude interface when LLDP enabled globally

Command Syntax

```
lldp (disable|enable) default-agent
```

Parameters

`disable`	Disables default LLDP agent
`enable`	Enables default LLDP agent

Command Mode

Interface mode

Applicability

This command is introduced from OcNOS version 5.0

Example

```
#configure terminal
(config)#interface xe1
(config-if)#lldp disable default-agent
(config-if)#lldp enable default-agent
```

lldp ip

Use this command to set the Link Layer Discovery Protocol with an IP address to be used as a chassis and management ID.

Use the `no` form of this command to remove this value.

Command Syntax

```
lldp ip address A.B.C.D
no lldp ip address
```

Parameters

`A.B.C.D`	Enter the IP address value

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#lldp ip address 1.1.1.1
(config)#no lldp ip address
```

lldp tlv

Use this command to set the TLVs enabled for transmission on a port. Make sure that the complete set of Type Length Values (TLVs) is specified when giving this command, because TLVs not specified are disabled.

Command Syntax

```
lldp tlv {chassis-id|port-id|ttl|port-description|system-name|system-
  description|system-capabilities|management-address|ieee-8021-org-specific|ieee-
  8023-org-specific}
```

Parameters

`chassis-id`	Chassis ID type length values (TLV)
`port-id`	Port ID TLV
`ttl`	Time to live TLV
`port-description`	Port description TLV
`system-name`	System name TLV
`system-description`	System Description
`system-capabilities`	System capabilities TLV
`management-address`	Management address TLV
`ieee-8021-org-specific`	IEEE 802.1 organizationally-specific TLV
`ieee-8023-org-specific`	IEEE 802.3 organizationally-specific TLV

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface eth0
(config-if)#lldp tlv chassis-id ieee-8021-org-specific ieee-8023-org-specific
management-address port-description port-id system-capabilities system-
description system-name ttl
```

set lldp chassis-id-tlv

Use this command to set the chassis ID subtype for the LLDP agent on a port.

Command Syntax

```
set lldp chassis-id-tlv (mac-address | ip-address)
```

Parameters

`mac-address`	Use the MAC address as the chassis ID
`ip-address`	Use the management IP address as the chassis ID

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp chassis-id-tlv ip-address
```

set lldp disable

Use this command to disable the LLDP agent on a port.

Command Syntax

```
set lldp disable
```

Parameters

None

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp disable
```

set lldp enable

Use this command to enables an LLDP agent on a port and specifies its type.

Command Syntax

```
set lldp enable (txonly|txrx|rxonly)
```

Parameters

`rxonly`	Receive-only
`txonly`	Transmit-only
`txrx`	Transmit and receive

Default

By default, no LLDP agent is enabled for a port.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth 0
(config-if)#set lldp enable rxonly
```

set lldp locally-assigned

Use this command to locally assign the LLDP Port ID and the Chassis ID TLV parameters.

Command Syntax

```
set lldp locally-assigned NAME
```

Parameters

NAME	Name assigned to the port.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth 0
(config-if)#set lldp locally-assigned port1
```

set lldp management-address-tlv

Use this command to set the management address subtype for the LLDP agent on a port.

Command Syntax

```
set lldp management-address-tlv (mac-address | ip-address)
```

Parameters

`mac-address`	Use the MAC address as the chassis ID
`ip-address`	Use the management IP address as the chassis ID

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth 0
(config-if)#set lldp management-address-tlv ip-address
```

set lldp msg-tx-hold

Use this command to set the `msg-tx-hold` parameter that determines the Time To Live (TTL) value for LLDPDUs to be transmitted by the port. The value set with this command is multiplied by the `lldp timer msg-tx-interval` value, which determines the final TTL value.

Command Syntax

```
set lldp msg-tx-hold VALUE
```

Parameters

`VALUE`	Time in seconds of LLDP msg-tx-hold

Default

The default value of the `lldp msg-tx-hold` parameter is 4 seconds.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config)#set lldp msg-tx-hold 3
```

set lldp system-description

Use this command to identify the string that describes the LLDP system.

Command Syntax

```
set lldp system-description LINE
```

Parameters

LINE	Set the description of the LLDP system.

Default

The default status of Ethernet OAM is disabled.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#set lldp system-description LLDP agent on B1
```

set lldp system-name

Use this command to identify the system name of the LLDP function.

Command Syntax

```
set lldp system-name NAME
```

Parameters

NAME	Name of the LLDP system.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#set lldp system-name LLDP1
```

set lldp timer

Use this command to set the interval at which LLDP frames are transmitted.

Command Syntax

```
set lldp timer msg-tx-interval <5-32768>
set lldp timer reinitDelay VALUE
set lldp timer tx-delay <1-8192>
```

Parameters

`msg-tx-interval`	
	Set the message transmit interval value
`<5-32768>`	Set the message transmit interval value
`reinitDelay`	Set the reinit delay value
`VALUE`	Set the reinit delay value
`tx-delay`	Set the transmit delay value
`<1-8192>`	Set the transmit delay value in range of:
	(1 <= `tx-delay` <= ((0.25)* `msg-tx-interval`)

Default Values

The default value for `msg-tx-interval` is 30 seconds.

The default value for `reinitDelay` is 2 seconds.

The default value of the `tx-delay` is 2 seconds.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#set lldp timer msg-tx-interval 40

#configure terminal
(config)#interface eth0
(config-if)#set lldp timer reinitDelay 3

#configure terminal
(config)#interface eth0
(config-if)#set lldp timer tx-delay 3
```

set lldp too-many-neighbors

Use this command to set the action to take when the remote table is full.

Command Syntax

```
set lldp too-many-neighbors limit <1-65535> discard received-info timer <1-65535>
set lldp too-many-neighbors limit <1-65535> discard existing-info MAC
  timer <1-65535>
```

Parameters

`limit`	The limit on the number of LLDP neighbors.
`<1-65535>`	The limit on the number of LLDP neighbors.
`received-info`	The information received for this neighbor.
`timer`	The period after which received information is discarded.
`<1-65535>`	The period in seconds after which received information is discarded.
`existing-info`	The information for this neighbor.
`MAC`	Identifies the remote LLDP Agent for which information is discarded.
`timer`	The period in seconds after which existing information is discarded.
`<1-65535>`	The period in seconds after which existing information is discarded.

Default Value

No upper limit is enforced for the number of remote LLDP agents.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#set lldp too-many-neighbors limit 20 disc existing-info 1.1.1.1.1
timer 1

(config)#interface eth1
(config-if)#set lldp too-many-neighbors limit 1 discard received-info timer 1
```

show lldp

Use this command to display LLDP port information.

Command Syntax

```
show lldp port IFNAME
show lldp port IFNAME statistics
```

Parameters

IFNAME	The name of the interface
statistics	Display LLDP port statistics

Command Mode

Exec mode and Privileged Exec mode

Example

The following sample output from this command displays detailed information about an LLDP-enabled port.

```
#show lldp port eth0
Remote LLDP
MAC Address: 01:06:29:CF:79:A1
TTL: 60
Network Address: 192.168.1.0
Interface Name: eth1
Interface Locally Assigned String: Port-a
Interface Description: bridge
Interface Number: 2
Port Vlan ID: 1
Protocol ID: 274242030202
AutoNego Support: Supported
AutoNego Capability: 1
Operational MAU Type: 3
Link Aggregation Status: Capable
Link Aggregation Port ID: 0
Max Frame Size: 128
System name:
System Description: bridge
System Capabilities: 4
System Capabilities Enabled: 4
```

The following sample output from this command displays all LLDP statistics for a selected port.

```
#show lldp port eth0 statistics
LLDP Port statistics for eth0
Frames transmitted: 22
Frames Aged out: 0
Frames Discarded: 0
Frames with Error: 0
Frames Received: 5
TLVs discarded: 0
TLVs unrecognized 0
```

snmp restart lldp

Use this command to restart SNMP in Link Layer Discovery Protocol (LLDP)

Command Syntax

```
snmp restart lldp
```

Parameters

None

Command Mode

Configure mode

Examples

```
#snmp restart lldp
```

Index

Numerics

A

B

C

D

E

G

I

L

T

U

V

W