Cisco 4-Port and 8-Port Layer 2 Gigabit EtherSwitch Network Interface Module Configuration Guide for Cisco 4000 Series ISR

First Published: May 6, 2015

The Cisco 4-Port and 8-Port Layer 2 Gigabit EtherSwitch Network Interface Module (NIM) integrates the Layer 2 features and provides a 1-Gbps connection to the multigigabit fabric (MGF) for intermodule communication.

The Cisco NIM-ES2-4 and Cisco NIM-ES2-8 are capable of providing up to 30 watts of power per port with the robust Power over Ethernet (POE), Power over Ethernet Plus (PoE+), and Enhanced Power over Ethernet (ePoE) features, which work on Cisco 4000 Series ISR families.

The following is the feature history for the Cisco 4-Ports and 8-Ports Layer 2 Gigabit EtherSwitch Network Interface Modules :

Table 1 Feature History for Cisco Layer 2/3 NIM

Release	Modification
Cisco IOS XE Release 3.15S (router software)	This feature was introduced

Finding Support Information for Platforms and Cisco IOS Software Images

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

Cisco Systems, Inc.
www.cisco.com

Prerequisites for the Cisco 4-Ports and 8-Ports Layer 2 Gigabit EtherSwitch Network Interface Modules

Cisco IOS XE Release 3.15S is required to install the Cisco NIM-ES2-4 or Cisco NIM-ES2-8.

To determine the version of Cisco IOS software that is running on your router, log in to the router and enter the **show version** command:

```
Router> show version
Cisco IOS XE Software, Version 03.15.00.S - Standard Support Release
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 15.5(2)S,
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Sun 22-Mar-15 02:32 by mcpre
```

- To view the router (Cisco 4000 Series ISR), Cisco IOS software release, and feature set, enter the **show version** command in privileged EXEC mode.
- To view the Cisco IOS Release number mapping, see *Release Notes for the Cisco ISR 4400 Series.*

Information About the Cisco 4-Ports and 8-Ports Layer 2 Gigabit EtherSwitch Network Interface Modules

This section describes the features and some important concepts about the Cisco NIM-ES2-4 and Cisco NIM-ES2-8:

Note For a list of Cisco IOS switch feature documentation with information on various supported features on your Cisco NIM-ES2-4 and Cisco NIM-ES2-8, see the Related Documentation, page 25

Hardware Overview

The Cisco 4-Ports and 8-Ports Layer 2 Gigabit EtherSwitch Network Interface Modules (Cisco NIM-ES2-4 and Cisco NIM-ES2-8) are switch modules to which you can connect Cisco IP phones, Cisco wireless access point workstations, and other network devices such as video devices, routers, switches, and other network switch modules.

The following Cisco 4-Ports and 8-Ports Layer 2 Gigabit EtherSwitch Network Interface Modules are supported on the Cisco 4000 Series ISRs:

- 4-port non-POE Layer 2 Gigabit Ethernet Switch Network Interface Module (NIM-ES2-4)
- 8-port non-POE Layer 2 Gigabit Ethernet Switch Network Interface Module (NIM-ES2-8)

- 8-port POE Layer 2 Gigabit Ethernet Switch Network Interface Module (NIM-ES2-8-P)

For complete information about the Cisco NIM-ES2-4 and Cisco NIM-ES2-8 hardware, see the *Installing the Cisco 4-Port and 8-Port Layer 2 Gigabit EtherSwitch Network Interface Module* guide.

Software Features

The following are the switching software features supported on the Cisco NIM-ES2-4 and Cisco NIM-ES2-8:

Assigning IP Addresses to Switch Virtual Interfaces

To configure IP routing, you need to assign IP addresses to Layer 3 network interfaces. This enables communication with the hosts on those interfaces that use IP. IP routing is disabled by default, and no IP addresses are assigned to Switch Virtual Interfaces (SVIs).

An IP address identifies a destination for IP packets. Some IP addresses are reserved for special uses and cannot be used for host, subnet, or network addresses. RFC 1166, “Internet Numbers,” contains the official description of these IP addresses.

An interface can have one primary IP address. A a subnet mask identifies the bits that denote the network number in an IP address.

Beginning in privileged EXEC mode, follow these steps to assign an IP address and a network mask to an SVI

	Command	Purpose
Step 1	`configure terminal`	Enter global configuration mode.
Step 2	`interface vlan` *vlan_id*	Enter interface configuration mode, and specify the Layer 3 VLAN to configure.
Step 3	`ip address` *ip-address subnet-mask*	Configure the IP address and IP subnet mask.
Step 4	`end`	Return to privileged EXEC mode.

	Command	Purpose
Step 5	**show interfaces** [*interface-id*] **show ip interface** [*interface-id*] **show running-config interface** [*interface-id*]	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

IEEE 802.1x Protocol

The IEEE 802.1x standard defines a client/server-based access control and authentication protocol that prevents clients from connecting to a LAN through publicly accessible ports unless they are authenticated. The authentication server authenticates each client connected to a port before making available any services offered by the router or the LAN.

Until the client is authenticated, IEEE 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication, normal traffic can pass through the port. See *Configuring IEEE 802.1X Port-Based Authentication* chapter in the *Cisco 7600 Series Router Software Configuration Guide, Cisco IOS Release 15S.*

IGMP Snooping for IPv4

IGMP snooping allows switches to examine IGMP packets and make forwarding decisions based on their content. You can configure the switch to use IGMP snooping in subnets that receive IGMP queries from either IGMP or the IGMP snooping querier. IGMP snooping constrains IPv4 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv4 multicast traffic only to those ports that want to receive it.

Layer 2 switches can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients. For more information on this feature, see http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/15-2_1_e/configuration/guide/scg3750x/swigmp.html.

Power over Ethernet (Plus)

The Cisco NIM-ES2-8-P supports POE (802.3af) and POE+(802.3at) on all its 8 ports. PoE provides up to 15.4 Watts of power, and PoE+ provides up to 30 Watts of power. By using PoE, you do not need to supply connected PoE- enabled devices with wall power. This eliminates the cost for additional electrical cabling that would otherwise be necessary for connected devices.

Note To ensure the PoE feature is functional, verify the availability of PoE power on your router using the **show platform** and **show power** commands.

The NIM-ES2-8-P PoE configuration is same as on ISR 4400 router FPGE ports. Please see Configuring PoE for FPGE Ports for how to configure PoE on NIM-ES2-8-P ports.

In this example, power is being supplied to an IP phone though NIM-ES2-8-P Gi0/1/1 port.

```
Router#show power inline
RAvailable:500.0(w)  Used:10.3(w)  Remaining:489.8(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi0/1/1   auto   on         10.3    IP Phone 7970       3     30.0
Gi0/1/2   off    off        0.0     n/a                 n/a   30.0
Gi0/1/3   auto   off        0.0     n/a                 n/a   30.0
Gi0/1/4   auto   off        0.0     n/a                 n/a   30.0
Gi0/1/5   auto   off        0.0     n/a                 n/a   30.0
Gi0/1/6   auto   off        0.0     n/a                 n/a   30.0
Gi0/1/7   auto   off        0.0     n/a                 n/a   30.0
Gi0/1/8   auto   off        0.0     n/a                 n/a   30.0.
```

Cisco Intelligent Power Management

The PDs and the switch negotiate power through CDP messages for an agreed power-consumption level. The negotiation allows high-power Cisco PDs to operate at their highest power mode.
The PoE plus feature enables automatic detection and power budgeting; the switch maintains a power budget, monitors, and tracks requests for power, and grants power only when it is available. See the *Configuring the External PoE Service Module Power Supply Mode* section in the *Catalyst 3560 Switch Software Configuration Guide, Cisco IOS Release 15.0(2)SE and Later.*

Power Policing (Sensing)

Power policing allows to monitor the real-time power consumption. On a per-PoE port basis, the switch senses the total power consumption, polices the power usage, and reports the power usage. For more information on this feature, see Related Documentation, page 25.

MAC Table Manipulation

This section includes the following:

Creating a Static Entry in the MAC Address Table

Perform the following task to create a static entry in the MAC address table.

MAC Address-Based Traffic Blocking

Perform the following task to block all traffic to or from a MAC address in a specified VLAN.

	Command	Purpose
Step 1	**enable** `Router# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** `Router#configure terminal`	Enters global configuration mode.
Step 3	**mac address-table static mac-address vlan vlan-id drop** `Router# mac address-table static mac-address vlan vlan-id drop`	Creates a static entry in the MAC address table.
Step 4	**end** `Router# end`	Returns to privileged EXEC mode.
Step 5	**show mac address-table** `Router# show mac address-table`	Verifies the MAC address table.

Configuring and Verifying the Aging Timer

Perform this task to configure the aging timer.

Spanning Tree Protocol

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing undesirable loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Spanning tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or to a switched LAN of multiple segments. For more information on this feature, see http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/geshwic_cfg.html.

Configuring the Switched Port Analyzer

This section describes how to configure a Switched Port Analyzer (SPAN) session on Cisco NIM-ES2-4 and Cisco NIM-ES2-8. The following restrictions apply to the Cisco NIM-ES2-4 and Cisco NIM-ES2-8:

- Only intra-module local SPAN is supported and cross module SPAN is not supported.
- Each NIM-ES2-4/8 supports only one local SPAN session.
- Each SPAN session supports only one source port and one destination port.

Note Tx, Rx, or both Tx and Rx monitoring is supported.

- Configuring the SPAN Sources, page 8
- Configuring SPAN Destinations, page 8
- Verifying the SPAN Session, page 8

- Removing Sources or Destinations from a SPAN Session, page 8

Configuring the SPAN Sources

To configure the source for a SPAN session, use the **monitor session** *session* **source** {**interface** *type 0/slot/port* | **vlan** *vlan_ID* [**,** | **-** | **rx** | **tx** | **both**]} command in global configuration mode. This command specifies the SPAN session, the source interfaces or VLANs, and the traffic direction to be monitored.

```
Router(config)# monitor session 1 source interface gigabitethernet 0/1/1
```

Configuring SPAN Destinations

To configure the destination for a SPAN session, use the **monitor session** *session* **destination** {**interface** *type slot/subslot/port* | **-** | **rx** | **tx** | **both**]} command in global configuration mode.

```
Router(config)# monitor session 1 destination interface gigabitethernet 0/1/1
```

Verifying the SPAN Session

Use the **show monitor session** command to verify the sources and destinations configured for the SPAN session.

```
Router#show monitor session 1
Session 1
---------
Session 1
---------
Type : Local Session
Source Ports :
Both : Gi0/1/0
Destination Ports : Gi0/1/1
```

Removing Sources or Destinations from a SPAN Session

To remove sources or destinations from the SPAN session, use the **no monitor session** *session* command in global configuration mode as shown in the following example:

```
Router(config)#no monitor session 1
```

Configuring Layer 2 Quality of Service

Cisco NIM-ES2-4 and Cisco NIM-ES2-8 supports four egress queues on each port for L2 data traffic. The four queues are strict priority queues by default, which is, queue one is lowest priority queue and queue four is highest priority queue. Shaped Deficit Weight Round Robin (SDWRR) is also supported and the weight of each queue can be configured.

The Cisco NIM-ES2-4 and Cisco NIM-ES2-8 L2 QoS configuration is a global configuration and it is not per module nor per port.

Configuring 802.1p COS-based queue mapping

Beginning in privileged EXEC mode, follow these steps to configure the CoS based queue mapping:

To disable the new CoS settings and return to default settings, use the **no wrr-queue cos-map** global configuration command.

Configuring SDWRR Priority

Beginning in privileged EXEC mode, follow these steps to configure the SDWRR priority:

	Command	Purpose
Step 1	`configure terminal`	Enter global configuration mode.
Step 2	`wrr-queue bandwidth weight1...weight4`	Assign SDWRR weights to the four CoS queues. The range for the WRR values weight1 through weight4 is 1 to 255.
Step 3	`end`	Return to privileged EXEC mode.
Step 4	`show wrr-queue bandwidth`	Display the SDWRR bandwidth allocation for the queues.

Note Once SDWRR priority is configured the SDWRR scheduling will be activated and strict priority will be disabled. To disable the SDWRR scheduling and enable the strict priority scheduling, use the **no wrr-queue bandwidth** global configuration command.

Configuring the CoS value for an Interface

Beginning in privileged EXEC mode, follow these steps to define the default CoS value of a port or to assign the default CoS to all incoming packets on the port:

To return to the default setting, use the **no switchport priority {default | override}** interface configuration command.

VLANs

Virtual local-area networks (VLANs) are a group of end stations with a common set of requirements, independent of physical location. VLANs have the same attributes as a physical LAN but allow you to group end stations even if they are not located physically on the same LAN segment. For more information on this feature, see http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/geshwic_cfg.html.

Configuring LAN Ports for Layer 2 Switching

This chapter describes how to use the command-line interface (CLI) to configure Gigabit Ethernet, and 10/100/1000-Gigabit Ethernet LAN ports for Layer 2 switching on the Cisco 4000 series routers. The configuration tasks in this section apply to LAN ports on LAN switching modules.

Layer 2 LAN Port Modes

Table 1-2 lists the Layer 2 LAN port modes and describes how they function on LAN ports.

Table 1-2 Layer 2 LAN Port Modes

Mode	Function
switchport mode access	Puts the LAN port into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The LAN port becomes a nontrunk port even if the neighboring LAN port does not agree to the change.
switchport mode dynamic desirable	Makes the LAN port actively attempt to convert the link to a trunk link. The LAN port becomes a trunk port if the neighboring LAN port is set to **trunk**, **desirable**, or **auto** mode. This is the default mode for all LAN ports.
switchport mode dynamic auto	Makes the LAN port willing to convert the link to a trunk link. The LAN port becomes a trunk port if the neighboring LAN port is set to **trunk** or **desirable** mode.
switchport mode trunk	Puts the LAN port into permanent trunking mode and negotiates to convert the link into a trunk link. The LAN port becomes a trunk port even if the neighboring port does not agree to the change.
switchport nonegotiate	Puts the LAN port into permanent trunking mode but prevents the port from generating DTP frames. You must configure the neighboring port manually as a trunk port to establish a trunk link.

Note DTP is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly. To avoid this problem, ensure that LAN ports connected to devices that do not support DTP are configured with the **access** keyword if you do not intend to trunk across those links. To enable trunking to a device that does not support DTP, use the **nonegotiate** keyword to cause the LAN port to become a trunk but not generate DTP frames.

Default Layer 2 LAN Interface Configuration

Table 1-3 shows the Layer 2 LAN port default configuration.

Table 1-3 Layer 2 LAN Interface Default Configuration

Feature	Default
Interface mode: • Before entering the **switchport** command • After entering the **switchport** command	 **switchport mode dynamic desirable**
Default access VLAN	VLAN 1
Native VLAN (for 802.1Q trunks)	VLAN 1

Configuring LAN Interfaces for Layer 2 Switching

These sections describe how to configure Layer 2 switching on the Cisco4000 series routers:

Note Use the **default interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/subslot/port* command to revert an interface to its default configuration.

Configuring a LAN Port for Layer 2 Switching

To configure a LAN port for Layer 2 switching, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface` *type*[1] *slot/subslot/port*	Selects the LAN port to configure.
Step 2	`Router(config-if)# shutdown`	(Optional) Shuts down the interface to prevent traffic flow until configuration is complete.
Step 3	`Router# show running-config interface` [*type*[1] *slot/port*]	Displays the running configuration of the interface.
Step 4	`Router# show interfaces` [*type*[1] *slot/subslot/port*] `switchport`	Displays the switch port configuration of the interface.
Step 5	`Router# show interfaces` [*type*[1] *slot/subslot/port*] `trunk`	Displays the trunk configuration of the interface.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

After you enter the **switchport** command, the default mode is **switchport mode dynamic desirable**. If the neighboring port supports trunking and is configured to allow trunking, the link becomes a Layer 2 trunk when you enter the **switchport** command. By default, LAN trunk ports negotiate encapsulation. If the neighboring port supports ISL and 802.1Q encapsulation and both ports are set to negotiate the encapsulation type, the trunk uses ISL encapsulation (10-Gigabit Ethernet ports do not support ISL encapsulation).

Configuring a Layer 2 Switching Port as a Trunk

These section describe configuring a Layer 2 switching port as a trunk:

Configuring the Layer 2 Switching Port as 802.1Q Trunk

Note
- Complete the steps in the "Configuring a LAN Port for Layer 2 Switching" section on page 12 before performing the tasks in this section.

- When you enter the **switchport** command with no other keywords, the default mode is **switchport mode dynamic desirable** and **switchport trunk encapsulation negotiate**.

To configure the Layer 2 switching port as an ISL or 802.1Q trunk, perform this task:

Command	Purpose
`Router(config-if)# switchport mode trunk`	(Optional) Configures the Layer 2 switching port mode as 802.1Q trunk.

When configuring the Layer 2 switching port as 802.1Q trunk, note the following information:

- The **switchport mode trunk** command (see the "Configuring the Layer 2 Trunk Not to Use DTP" section on page 13) is not compatible with the **switchport trunk encapsulation negotiate** command.
- To support the **switchport mode trunk** command, you must configure the encapsulation as 802.1Q.

Configuring the Layer 2 Trunk to Use DTP

Note Complete the steps in the "Configuring a LAN Port for Layer 2 Switching" section on page 12 before performing the tasks in this section.

To configure the Layer 2 trunk to use DTP, perform this task:

Command	Purpose
`Router(config-if)# switchport mode dynamic {auto | desirable}`	(Optional) Configures the trunk to use DTP.
`Router(config-if)# no switchport mode`	Reverts to the default trunk trunking mode (**switchport mode dynamic desirable**).

When configuring the Layer 2 trunk to use DTP, note the following information:

- Required only if the interface is a Layer 2 access port or to specify the trunking mode.
- See Table 1-2 on page 11 for information about trunking modes.

Configuring the Layer 2 Trunk Not to Use DTP

Note Complete the steps in the "Configuring a LAN Port for Layer 2 Switching" section on page 12 before performing the tasks in this section.

To configure the Layer 2 trunk not to use DTP, perform this task:

	Command	Purpose
Step 1	`Router(config-if)# switchport mode trunk`	(Optional) Configures the port to trunk unconditionally.
	`Router(config-if)# no switchport mode`	Reverts to the default trunk trunking mode (**switchport mode dynamic desirable**).
Step 2	`Router(config-if)# switchport nonegotiate`	(Optional) Configures the trunk not to use DTP.
	`Router(config-if)# no switchport nonegotiate`	Enables DTP on the port.

When configuring the Layer 2 trunk not to use DTP, note the following information:

- Before entering the **switchport mode trunk** command, you must configure the encapsulation (see the "Configuring the Layer 2 Switching Port as 802.1Q Trunk" section on page 12).
- To support the **switchport nonegotiate** command, you must enter the **switchport mode trunk** command.
- Enter the **switchport mode dynamic trunk** command. See Table 1-2 on page 11 for information about trunking modes.
- Before entering the **switchport nonegotiate** command, you must configure the encapsulation (see the "Configuring the Layer 2 Switching Port as 802.1Q Trunk" section on page 12) and configure the port to trunk unconditionally with the **switchport mode trunk** command (see the "Configuring the Layer 2 Trunk to Use DTP" section on page 13).

Configuring the Access VLAN

Note Complete the steps in the "Configuring a LAN Port for Layer 2 Switching" section on page 12 before performing the tasks in this section.

To configure the access VLAN, perform this task:

Configuring the 802.1Q Native VLAN

Command	Purpose
`Router(config-if)# switchport access vlan` *vlan_ID*	(Optional) Configures the access VLAN, which is used if the interface stops trunking. The *vlan_ID* value can be 1 through 4094, except reserved VLANs.
`Router(config-if)# no switchport access vlan`	Reverts to the default value (VLAN 1).

Note Complete the steps in the "Configuring a LAN Port for Layer 2 Switching" section on page 12 before performing the tasks in this section.

To configure the 802.1Q native VLAN, perform this task:

Command	Purpose
`Router(config-if)# switchport trunk native vlan vlan_ID`	(Optional) Configures the 802.1Q native VLAN.
`Router(config-if)# no switchport trunk native vlan`	Reverts to the default value (VLAN 1).

When configuring the native VLAN, note the following information:

- The *vlan_ID* value can be 1 through 4094, except reserved VLANs.
- The access VLAN is not automatically used as the native VLAN.

Configuring the List of VLANs Allowed on a Trunk

Note Complete the steps in the "Configuring a LAN Port for Layer 2 Switching" section on page 12 before performing the tasks in this section.

To configure the list of VLANs allowed on a trunk, perform this task:

Command	Purpose
`Router(config-if)# switchport trunk allowed vlan {add | except | none | remove} vlan [,vlan[,vlan[,...]]`	(Optional) Configures the list of VLANs allowed on the trunk.
`Router(config-if)# no switchport trunk allowed vlan`	Reverts to the default value (all VLANs allowed).

When configuring the list of VLANs allowed on a trunk, note the following information:

- The *vlan* parameter is either a single VLAN number from 1 through 4094, or a range of VLANs described by two VLAN numbers, the lesser one first, separated by a dash. Do not enter any spaces between comma-separated *vlan* parameters or in dash-specified ranges.
- All VLANs are allowed by default.
- You can remove VLAN 1. If you remove VLAN 1 from a trunk, the trunk interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), Port Aggregation Protocol (PAgP), and DTP in VLAN 1.

STP Overview

STP is a Layer 2 link-management protocol that provides path redundancy while preventing undesirable loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. STP operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

Cisco 4-Ports and 8-Ports Layer 2 Gigabit EtherSwitch Network Interface Modules use STP (the IEEE 802.1D bridge protocol) on all VLANs. By default, a single instance of STP runs on each configured VLAN (provided you do not manually disable STP). You can enable and disable STP on a per-VLAN basis.

Cisco 4-Ports and 8-Ports Layer 2 Gigabit EtherSwitch Network Interface Modules support the following three STP:

- Multiple Spanning Tree protocol, page 16
- Per-VLAN Spanning Tree+, page 16
- Rapid Per-VLAN Spanning Tree+, page 16

Multiple Spanning Tree protocol

MST maps multiple VLANs into a spanning tree instance, with each instance having a spanning tree topology independent of other spanning tree instances. This architecture provides multiple forwarding paths for data traffic, enables load balancing, and reduces the number of spanning tree instances required to support a large number of VLANs. MST improves the fault tolerance of the network because a failure in one instance (forwarding path) does not affect other instances (forwarding paths).

Per-VLAN Spanning Tree+

Per-VLAN Spanning Tree+ (PVST+) is an extension of the PVST standard. Per-VLAN Spanning Tree+ (PVST+) allows interoperability between CST and PVST in Cisco switches and supports the IEEE 802.1Q standard.

Rapid Per-VLAN Spanning Tree+

Rapid-PVST uses the existing configuration for PVST+; however, Rapid-PVST uses RSTP to provide faster convergence. Independent VLANs run their own RSTP instance. Dynamic entries are flushed immediately on a per-port basis upon receiving a topology change. UplinkFast and BackboneFast configurations are ignored in Rapid-PVST mode; both features are included in RSTP.

Default STP Configuration

Table 1-4 shows the default STP configuration.

Table 1-4 STP Default Configuration

Feature	Default Value
Disable state	STP disabled for all VLANs
Bridge priority	32768
STP port priority (configurable on a per-port basis—used on LAN ports configured as Layer 2 access ports)	128
STP port cost (configurable on a per-port basis—used on LAN ports configured as Layer 2 access ports)	Gigabit Ethernet: 4
STP VLAN port priority (configurable on a per-VLAN basis—used on LAN ports configured as Layer 2 trunk ports)	128

Table 1-4 STP Default Configuration (continued)

Feature	Default Value
STP VLAN port cost (configurable on a per-VLAN basis—used on LAN ports configured as Layer 2 trunk ports)	Gigabit Ethernet:1000000000
Hello time	2 seconds
Forward delay time	15 seconds
Maximum aging time	20 seconds
Mode	PVST

Enabling STP

Note STP is disabled by default on all VLANs.

You can enable STP on a per-VLAN basis. The Cisco 4-Ports and 8-Ports Layer 2 Gigabit EtherSwitch Network Interface Modules maintain a separate instance of STP for each VLAN (except on VLANs on which you disable STP).

To enable STP on a per-VLAN basis, perform this task:

	Command	Purpose
Step 1	`Router(config)# spanning-tree vlan vlan_ID`	Enables STP on a per-VLAN basis. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 1-4 on page 16).
	`Router(config)# default spanning-tree vlan vlan_ID`	Reverts all STP parameters to default values for the specified VLAN.
	`Router(config)# no spanning-tree vlan vlan_ID`	Disables STP on the specified VLAN; see the following Cautions for information regarding this command.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show spanning-tree vlan vlan_ID`	Verifies that STP is enabled.

Caution Do not disable spanning tree on a VLAN unless all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the VLAN. This action can have unexpected results because switches and bridges with spanning tree enabled will have incomplete information regarding the physical topology of the network.

Caution We do not recommend disabling spanning tree, even in a topology that is free of physical loops. Spanning tree serves as a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.

This example shows how to enable STP on VLAN 200:

```
Router# configure terminal
Router(config)# spanning-tree vlan 200
Router(config)# end
Router#
```

Note STP is disabled by default.

This example shows how to verify the configuration:

```
Router# show spanning-tree vlan 200

G0:VLAN0200
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     00d0.00b8.14c8
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768
              Address     00d0.00b8.14c8
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Gi1/4            Desg FWD 200000    128.196  P2p
Gi1/5            Back BLK 200000    128.197  P2p

Router#
```

Note You must have at least one interface that is active in VLAN 200 to create a VLAN 200 spanning tree. In this example, two interfaces are active in VLAN 200.

Configuring Optional STP Features

This section describes how to configure the following optional STP features:

Enabling PortFast

Caution Use PortFast *only* when connecting a single end station to a Layer 2 access port. Otherwise, you might create a network loop.

To enable PortFast on a Layer 2 access port, perform this task:

This example shows how to enable PortFast on Gigabit Ethernet interface 1:

```
Router# configure terminal
Router(config)# interface GigabitEthernet 1
Router(config-if)# spanning-tree portfast
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show running-config interface fastethernet 5/8
Building configuration...

Current configuration:
!
interface GigabitEthernet1
 no ip address
 switchport
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
end

Router#
```

To enable the default PortFast configuration, perform this task:

	Command	Purpose
Step 1	`Router(config)# spanning-tree portfast default`	Configures the PortFast default.
Step 2	`Router(config)# show spanning-tree summary totals`	Verifies the global configuration.
Step 3	`Router(config)# show spanning-tree interface` *x* **detail**	Verifies the effect on a specific port.
Step 4	`Router(config-if)# spanning-tree portfast trunk`	Enables the PortFast trunk on a port
Step 5	`Router# show spanning-tree interface fastEthernet` *x* **detail**	Verifies the configuration.

This example shows how to enable the default PortFast configuration:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# spanning-tree portfast default
Router(config)# ^Z

Root bridge for:VLAN0010
EtherChannel misconfiguration guard is enabled
Extended system ID   is disabled
```

```
Portfast              is enabled by default
PortFast BPDU Guard   is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard             is disabled by default
UplinkFast            is disabled
BackboneFast          is disabled
Pathcost method used is long

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                  0        0         0        1          1
VLAN0010                  0        0         0        2          2
---------------------- -------- --------- -------- ---------- ----------
2 vlans                   0        0         0        3          3
Router#

Router# show spanning-tree interface GigabitEthernet 0/1/0 detail
Port 17 (GigabitEthernet0/1/0) of G0:VLAN0020 is forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.17.
   Designated root has priority 32788, address f44e.05da.bb11
   Designated bridge has priority 32788, address f44e.05da.bb11
   Designated port id is 128.17, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 61, received 0
Router(config-if)# spanning-tree portfast trunk
%Warning:portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
```

Enabling PortFast BPDU Filtering

These sections describe how to configure PortFast BPDU filtering.

To enable PortFast BPDU filtering globally, perform this task:

	Command	Purpose
Step 1	`Router(config)# spanning-tree portfast bpdufilter default`	Enables BPDU filtering globally on the router.
Step 2	`Router# show spanning-tree summary totals`	Verifies the configuration.

BPDU filtering is set to default on each port. This example shows how to enable PortFast BPDU filtering on the port and verify the configuration in PVST+ mode:

```
Router(config)# spanning-tree portfast bpdufilter default
Router(config)# ^Z

Router# show spanning-tree summary totals
Switch is in pvst mode
Root bridge for: G0:VLAN0013, G0:VLAN0020, G1:VLAN0020
EtherChannel misconfig guard is enabled
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
```

```
Loopguard Default            is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Pathcost method used         is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
3 vlans                       0         0        0          3          3
```

To enable PortFast BPDU filtering on a nontrunking port, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface fastEthernet 4/4`	Selects the interface to configure.
Step 2	`Router(config-if)# spanning-tree bpdufilter enable`	Enables BPDU filtering.
Step 3	`Router# show spanning-tree interface fastEthernet 4/4`	Verifies the configuration.

This example shows how to enable PortFast BPDU filtering on a nontrunking port:

```
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree bpdufilter enable
Router(config-if)# ^Z

Router# show spanning-tree interface fastEthernet 4/4

Vlan             Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
VLAN0010         Desg FWD 1000      160.196  Edge P2p
Router# show spanning-tree interface fastEthernet 4/4 detail
Router# show spanning-tree interface fastEthernet 4/4 detail
 Port 196 (FastEthernet4/4) of VLAN0010 is forwarding
   Port path cost 1000, Port priority 160, Port Identifier 160.196.
   Designated root has priority 32768, address 00d0.00b8.140a
   Designated bridge has priority 32768, address 00d0.00b8.140a
   Designated port id is 160.196, designated path cost 0
   Timers:message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state:1
   The port is in the portfast mode by portfast trunk configuration
   Link type is point-to-point by default
   Bpdu filter is enabled
   BPDU:sent 0, received 0
Router#
```

Enabling BPDU Guard

To enable BPDU Guard globally, perform this task:

	Command	Purpose
Step 1	`Router(config)# spanning-tree portfast bpduguard default` `Router(config)# no spanning-tree portfast bpduguard default`	Enables BPDU Guard globally. Disables BPDU Guard globally.

	Command	Purpose
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show spanning-tree summary totals`	Verifies the configuration.

This example shows how to enable BPDU Guard:

```
Router# configure terminal
Router(config)# spanning-tree portfast bpduguard
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree summary totals default
Root bridge for:VLAN0010
EtherChannel misconfiguration guard is enabled
Extended system ID   is disabled
Portfast             is enabled by default
PortFast BPDU Guard  is disabled by default
Portfast BPDU Filter is enabled by default
Loopguard            is disabled by default
UplinkFast           is disabled
BackboneFast         is disabled
Pathcost method used is long

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
2 vlans                   0        0         0        3          3
Router#
```

Enabling UplinkFast

UplinkFast increases the bridge priority to 49152 and adds 3000 to the STP port cost of all Layer 2 LAN interfaces on the Cisco 7600 series router, decreasing the probability that the router will become the root bridge. The *max_update_rate* value represents the number of multicast packets transmitted per second (the default is 150 packets per second). UplinkFast cannot be enabled on VLANs that have been configured for bridge priority. To enable UplinkFast on a VLAN with bridge priority configured, restore the bridge priority on the VLAN to the default value by entering a **no spanning-tree vlan** *vlan_ID* **priority** command in global configuration mode.

Note When you enable UplinkFast, it affects all VLANs on the Cisco 7600 series router. You cannot configure UplinkFast on an individual VLAN.

To enable UplinkFast, perform this task:

	Command	Purpose
Step 1	`Router(config)# spanning-tree uplinkfast [max-update-rate max_update_rate]`	Enables UplinkFast.
	`Router(config)# no spanning-tree uplinkfast max-update-rate`	Reverts to the default rate.
	`Router(config)# no spanning-tree uplinkfast`	Disables UplinkFast.

	Command	Purpose
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show spanning-tree vlan vlan_ID`	Verifies that UplinkFast is enabled.

This example shows how to enable UplinkFast with an update rate of 400 packets per second:

```
Router# configure terminal
Router(config)# spanning-tree uplinkfast max-update-rate 400
Router(config)# exit
Router#
```

This example shows how to verify that UplinkFast is enabled:

```
Router# show spanning-tree uplinkfast
UplinkFast is enabled
Router#
```

Enabling BackboneFast

Note BackboneFast operates correctly only when enabled on all network devices in the network. BackboneFast is not supported on Token Ring VLANs. This feature is supported for use with third-party network devices.

To enable BackboneFast, perform this task:

	Command	Purpose
Step 1	`Router(config)# spanning-tree backbonefast`	Enables BackboneFast.
	`Router(config)# no spanning-tree backbonefast`	Disables BackboneFast.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show spanning-tree vlan vlan_ID`	Verifies that UplinkFast is enabled.

This example shows how to enable BackboneFast:

```
Router# configure terminal
Router(config)# spanning-tree backbonefast
Router(config)# end
Router#
```

This example shows how to verify that BackboneFast is enabled:

```
Router# show spanning-tree backbonefast
BackboneFast is enabled

BackboneFast statistics
-----------------------
Number of transition via backboneFast (all VLANs) : 0
Number of inferior BPDUs received (all VLANs)     : 0
Number of RLQ request PDUs received (all VLANs)   : 0
Number of RLQ response PDUs received (all VLANs)  : 0
Number of RLQ request PDUs sent (all VLANs)       : 0
Number of RLQ response PDUs sent (all VLANs)      : 0
Router#
```

Managing the Cisco NIM ES2-4 and Cisco NIM ES2-8 Using OIR

This section provides information on managing the Cisco NIM-ES2-4 and Cisco NIM-ES2-8 on the Cisco 4000 Series ISR using OIR. The online insertion and removal (OIR) feature allows you to insert or remove your Cisco NIM-ES2-4 and Cisco NIM-ES2-8 from a Cisco 4000 series ISR without powering down the module. This process is also referred to as a surprise or hard OIR. The Cisco 4000 series ISR also supports any-to-any OIR, which means that a Network Interface Module (NIM) in a slot can be replaced by another NIM using the OIR feature.

When a module is inserted, power is available on the NIM, and it initializes itself to start functioning. The hot-swap functionality allows the system to determine when a change occurs in the unit's physical configuration and to reallocate the unit's resources to allow all interfaces to function adequately. This feature allows interfaces on the NIM to be reconfigured while other interfaces on the router remain unchanged. The software performs the necessary tasks involved in handling the removal and insertion of the NIM.

You can choose to gracefully power down your Cisco NIM-ES2-4 and Cisco NIM-ES2-8 before removing it from router. This type of OIR is also known as managed OIR or soft OIR. The managed OIR feature allows you to stop the power supply to your module using the **hw-module subslot [stop]** command and remove the module from one of the subslots while other active modules remain installed on the router.

Note If you are not planning to immediately replace a module after performing OIR, ensure that you install a blank filter plate in the subslot.

The **stop** option allows you to gracefully deactivate a module; the module is rebooted when the **start** option of the command is executed. The **reload** option will stop or deactivate a specified module and restart it.

Example

This section provides the sample output for thee **hw-module subslot** *slot/subslot* **reload** command. The following example shows what appears when you enter the **hw-module subslot** *slot-number/subslot-number* **reload** command:

```
Router# hw-module subslot 0/1 reload
Proceed with reload of module? [confirm]y
*Mar 30 05:17:19.814: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(NIM-ES2-8) reloaded on subslot 0/1
*Mar 30 05:17:19.816: %SPA_OIR-6-OFFLINECARD: SPA (NIM-ES2-8) offline in subslot 0/1
*Mar 30 05:17:21.810: %LINK-3-UPDOWN: Interface Vlan20, changed state to down
*Mar 30 05:17:22.810: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed
state to down
*Mar 30 05:17:28.176: %IOSXE-4-PLATFORM: R0/0: kernel: pci 0000:48:00.0: no hotplug
settings from platform
*Mar 30 05:17:32.071: %SPA_OIR-6-ONLINECARD: SPA (NIM-ES2-8) online in subslot 0/1
*Mar 30 05:17:34.051: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/0, changed state to
down
*Mar 30 05:17:36.739: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/0, changed state to up
*Mar 30 05:17:37.739: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1/0, changed state to up
```

Related Documentation

Related Topic	Document Title
Hardware installation instructions for Cisco NIM-ES2-4/8	*Installing the Cisco 4-Port and 8-Port Layer 2 Gigabit EtherSwitch Network Interface Module*
General information about configuration and command reference.	*Software Configuration Guide for the Cisco 4000 Integrated Services Router*
Regulatory compliance information for Cisco 4000 ISR.	*Regulatory Compliance and Safety Information for the Cisco 4000 Integrated Services Router*
Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2	*Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2*

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml