Layer 2 Switching Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches

First Published: July 2013
Last Updated: January 2015

Cisco Systems, Inc.
www.cisco.com

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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

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

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

CONTENTS

CHAPTER 15

CHAPTER 16

CHAPTER 1

Overview

This document describes how to configure Layer 2 switching features on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid switches, hereafter referred to as *switch*.

The switch has two different types of interfaces by default: network node interfaces (NNIs) to connect to the service provider network and user network interfaces (UNIs) to connect to customer networks. Some features are supported only on one of these port types. You can also configure enhanced network interfaces (ENIs). An ENI is typically a user-network facing interface and has the same default configuration and functionality as UNIs, but can be configured to support protocol control packets for Cisco Discovery Protocol (CDP), Spanning-Tree Protocol (STP), Link Layer Discovery Protocol (LLDP), and EtherChannel Link Aggregation Control Protocol (LACP) or Port Aggregation Protocol (PAgP).

This chapter provides an overview of the following Layer 2 switching features:

- VTP, page 1-2
- VLANs, page 1-2
- VLAN Trunks, page 1-3
- Asymmetric VLAN Mapping, page 1-3
- VMPS, page 1-3
- Private VLANs, page 1-3
- IEEE 802.1Q Tunneling, page 1-4
- VLAN Mapping, page 1-4
- Layer 2 Protocol Tunneling, page 1-4
- STP, page 1-5
- MSTP, page 1-5
- Optional STP Features, page 1-6
- REP, page 1-6
- UDLD, page 1-7
- Voice VLAN, page 1-7

VTP

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

Before you create VLANs, you must decide whether to use VTP in your network. Using VTP, you can make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network. Without VTP, you cannot send information about VLANs to other switches.

VTP is designed to work in an environment where updates are made on a single switch and are sent through VTP to other switches in the domain. It does not work well in a situation where multiple updates to the VLAN database occur simultaneously on switches in the same domain, which would result in an inconsistency in the VLAN database.

Related Topics

Chapter 2, “Configuring VLAN Trunking Protocol”

VLANs

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router.

The VLAN feature on the switch provides the following:

- Support for up to 1005 VLANs for assigning users to VLANs associated with appropriate network resources, traffic patterns, and bandwidth.
- Support for VLAN IDs in the full 1 to 4094 range allowed by the 802.1Q standard.
- VLAN Query Protocol (VQP) for dynamic VLAN membership.
- 802.1Q trunking encapsulation on all ports for network moves, adds, and changes; management and control of broadcast and multicast traffic; and network security by establishing VLAN groups for high-security users and network resources.
- VLAN 1 minimization for reducing the risk of spanning-tree loops or storms by allowing VLAN 1 to be disabled on any individual VLAN trunk link. With this feature enabled, no user traffic is sent or received on the trunk. The switch CPU continues to send and receive control protocol frames.
- UNI-ENI isolated VLANs to isolate customer VLANs from VLANs of other customers on the same switch. Local switching does not occur among UNIs or ENIs on the switch that belong to the same UNI-ENI isolated VLAN.
- Port security on a PVLAN host to limit the number of MAC addresses learned on a port, or define which MAC addresses may be learned on a port.
- VLAN Flex Link Load Balancing to provide Layer 2 redundancy without requiring Spanning Tree Protocol (STP). A pair of interfaces configured as primary and backup links can load balance traffic based on VLAN.

Related Topics

Chapter 3, “Configuring VLANs”

VLAN Trunks

A trunk is a point-to-point link between one or more Ethernet switch interfaces and another networking device such as a router or a switch. Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network. The switch supports the 802.1Q industry-standard trunking encapsulation.

Related Topics

Chapter 4, “Configuring VLAN Trunks”

Asymmetric VLAN Mapping

The Asymmetric VLAN mapping feature provides a method for restricting traffic on VLAN trunk ports. This feature lets you specify lists of VLANs that are allowed to forward traffic on the trunk port in the ingress direction, egress direction, or in both directions. This feature is supported on the CGS 2520 only.

This feature is useful in a utility substation environment where a VLAN trunk is connected between a Cisco CGS 2520 switch and an intelligent electronic device (IED). The trunk port on the Cisco CGS 2520 can be configured to allow ingress traffic for a given VLAN, such as generic object oriented substation events (GOOSE) messages from the IED, and the trunk port can be configured to allow traffic for specific VLAN IDs in the egress direction, allowing the IED to subscribe to GOOSE messages with those VLAN IDs. All other VLAN traffic on the trunk port can be blocked.

Related Topics

Chapter 5, “Configuring Asymmetric VLAN Mapping”

VMPS

Each time the client switch receives the MAC address of a new host, it sends a VLAN Query Protocol (VQP) query to the VLAN Membership Policy Server (VMPS). The query includes the newly seen MAC address and the port on which it was seen. When the VMPS receives this query, it searches its database for a MAC-address-to-VLAN mapping. The VMPS responds with a VLAN assignment for the port.

The switch cannot be a VMPS server but can act as a client to the VMPS and communicate with it through VQP.

Related Topics

Chapter 6, “Configuring VMPS”

Private VLANs

The private-VLAN feature addresses two problems that service providers face when using VLANs:

- Scalability: The switch supports up to 1005 active VLANs. If a service provider assigns one VLAN per customer, this limits the numbers of customers that the service provider can support.
- To enable IP routing, each VLAN is assigned a subnet address space or a block of addresses, which can waste the unused IP addresses and cause IP address management problems.

Using private VLANs addresses the scalability problem and provides IP address management benefits for service providers and Layer 2 security for customers.

Related Topics

Chapter 7, "Configuring Private VLANs"

IEEE 802.1Q Tunneling

802.1Q tunneling enables service providers to offer multiple point Layer 2 VPN services to customers.

Business customers of service providers often have specific requirements for VLAN IDs and the number of VLANs to be supported. The VLAN ranges required by different customers in the same service-provider network might overlap, and traffic of customers through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations and could easily exceed the VLAN limit (4096) of the 802.1Q specification.

Using the 802.1Q tunneling (QinQ) feature, service providers can use a single VLAN to support customers who have multiple VLANs. Customer VLAN IDs (C-VLANs) are preserved, and traffic from different customers is segregated within the service-provider network, even when they appear to be in the same VLAN. Using 802.1Q tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy and retagging the tagged packets.

Related Topics

Chapter 8, "Configuring IEEE 802.1Q Tunneling"

VLAN Mapping

VLAN mapping (or VLAN ID translation) on trunk ports connected to a customer network maps customer VLANs to service-provider VLANs. Packets entering the port are mapped to a service provider VLAN (S-VLAN) based on the port number and the original customer VLAN-ID (C-VLAN) of the packet. Because the VLAN ID is mapped to the S-VLAN on ingress, on the switch all forwarding operations are performed by using S-VLAN information and not C-VLAN information. Symmetrical mapping back to the C-VLAN occurs when packets exit the port.

Related Topics

Chapter 9, "Configuring VLAN Mapping"

Layer 2 Protocol Tunneling

Layer 2 protocol tunneling enables customers to control protocols such as BPDU, CDP, VTP, PAgP, LACP, and UDLD protocols to be tunneled across service-provider networks.

When protocol tunneling is enabled, edge switches on the inbound side of the service-provider network encapsulate Layer 2 protocol packets with a special MAC address and send them across the service-provider network. Core switches in the network do not process these packets but forward them as normal packets. Layer 2 protocol data units (PDUs) for CDP, STP, or VTP cross the service-provider network and are delivered to customer switches on the outbound side of the service-provider network. Identical packets are received by all customer ports on the same VLANs with these results:

- Users on each of a customer's sites can properly run STP, and every VLAN can build a correct spanning tree based on parameters from all sites and not just from the local site.
- CDP discovers and shows information about the other Cisco devices connected through the service-provider network.
- VTP provides consistent VLAN configuration throughout the customer network, propagating to all switches through the service provider that support VTP.

Related Topics

Chapter 10, "Configuring Layer 2 Protocol Tunneling"

STP

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Switches might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network. Spanning-tree 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.

The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology.

STP is supported by default on NNIs, can be enabled on ENIs, and is not supported on UNIs. STP has these features:

- Up to 128 supported spanning-tree instances
- Per-VLAN spanning-tree plus (PVST+) for balancing load across VLANs
- Rapid PVST+ for balancing load across VLANs and providing rapid convergence of spanning-tree instances

Related Topics

Chapter 11, "Configuring STP"

MSTP

802.1s Multiple Spanning Tree Protocol (MSTP) enables multiple VLANs to be mapped to the same spanning-tree instance, thereby reducing the number of spanning-tree instances needed to support a large number of VLANs. The MSTP provides for multiple forwarding paths for data traffic and enables load balancing. It improves the fault tolerance of the network because a failure in one instance (forwarding path) does not affect other instances (forwarding paths). The most common initial deployment of MSTP is in the backbone and distribution layers of a Layer 2 switched network. This deployment provides the highly available network required in a service-provider environment.

When the switch is in MST mode, the Rapid Spanning Tree Protocol (RSTP), which is based on 802.1w, is automatically enabled. The RSTP provides rapid convergence of the spanning tree through explicit handshaking that eliminates the 802.1D forwarding delay and quickly transitions root ports and designated ports to the forwarding state.

Related Topics

Chapter 12, "Configuring MSTP"

Optional STP Features

The following optional spanning-tree features are available in PVST+, rapid-PVST+, and MSTP modes on NNIs and ENIs where spanning tree has been enabled:

- Port Fast for eliminating the forwarding delay by enabling a spanning-tree port to immediately transition from the blocking state to the forwarding state
- Bridge protocol data unit (BPDU) guard for shutting down Port Fast-enabled ports that receive BPDUs
- BPDU filtering for preventing a Port Fast-enabled ports from sending or receiving BPDUs
- Root guard for preventing switches outside the network core from becoming the spanning-tree root
- Loop guard for preventing alternate or root port NNIs or ENIs from becoming designated ports because of a failure that leads to a unidirectional link

Related Topics

Chapter 13, "Configuring Optional Spanning-Tree Features"

REP

Resilient Ethernet Protocol (REP) is a Cisco proprietary protocol that provides an alternative to Spanning Tree Protocol (STP) to control network loops, to respond to link failures, and to improve convergence time. REP controls a group of ports connected in a segment, ensures that the segment does not create any bridging loops, and responds to link failures within the segment. REP provides a basis for constructing more complex networks and supports VLAN load balancing.

Related Topics

Chapter 14, "Configuring Resilient Ethernet Protocol"

UDLD

UDLD is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. All connected devices must support UDLD for the protocol to successfully identify and disable unidirectional links. When UDLD detects a unidirectional link, it disables the affected port and alerts you. Unidirectional links can cause a variety of problems, including spanning-tree topology loops.

Related Topics

Chapter 15, "Configuring UDLD"

Voice VLAN

The Voice VLAN feature enables access ports on the switch to carry IP voice traffic from a Cisco IP phone. Voice VLAN supports users connecting to both a Cisco IP phone and another data device, such as a PC, through the IP phone to a switch port. The voice traffic and data traffic can be treated differently with voice traffic having higher priority.

Related Topics

Chapter 16, "Configuring Voice VLAN"

Configuring VLAN Trunking Protocol

This chapter describes how to use the VLAN Trunking Protocol (VTP) and the VLAN database for managing VLANs with the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*.

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 2-22.

This chapter includes the following sections:

Information About VTP

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

Before you create VLANs, you must decide whether to use VTP in your network. Using VTP, you can make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network. Without VTP, you cannot send information about VLANs to other switches.

VTP is designed to work in an environment where updates are made on a single switch and are sent through VTP to other switches in the domain. It does not work well in a situation where multiple updates to the VLAN database occur simultaneously on switches in the same domain, which would result in an inconsistency in the VLAN database.

The switch supports VLANs, but the number of configured features affects the usage of the switch hardware. If the switch is notified by VTP of a new VLAN and the switch is already using the maximum available hardware resources, it sends a message that there are not enough hardware resources available and shuts down the VLAN. The output of the **show vlan** user EXEC command shows the VLAN in a suspended state.

VTP version 1 and version 2 support only normal-range VLANs (VLAN IDs 1 to 1005). Cisco IOS Release 12.2(52)SE and later support VTP version 3. VTP version 3 supports the entire VLAN range (VLANs 1 to 4094). Extended range VLANs (VLANs 1006 to 4094) are supported only in VTP version 3. You cannot convert from VTP version 3 to VTP version 2 if extended VLANs are configured in the domain.

This section includes the following topics:

- VTP Domain, page 2-2
- VTP Modes, page 2-3
- VTP Advertisements, page 2-4
- VTP Version 2, page 2-4
- VTP Version 3, page 2-5
- VTP Pruning, page 2-6

VTP Domain

A VTP domain (also called a VLAN management domain) consists of one switch or several interconnected switches under the same administrative responsibility sharing the same VTP domain name. A switch can be in only one VTP domain. You make global VLAN configuration changes for the domain.

By default, the switch is in the VTP no-management-domain state until it receives an advertisement for a domain over a trunk link (a link that carries the traffic of multiple VLANs) or until you configure a domain name. Until the management domain name is specified or learned, you cannot create or modify VLANs on a VTP server, and VLAN information is not propagated over the network.

If the switch receives a VTP advertisement over a trunk link, it inherits the management domain name and the VTP configuration revision number. The switch then ignores advertisements with a different domain name or an earlier configuration revision number.

Caution Before adding a VTP client switch to a VTP domain, always verify that its VTP configuration revision number is *lower* than the configuration revision number of the other switches in the VTP domain. Switches in a VTP domain always use the VLAN configuration of the switch with the highest VTP configuration revision number. If you add a switch that has a revision number higher than the revision number in the VTP domain, it can erase all VLAN information from the VTP server and VTP domain. Refer to the "Adding a VTP Client Switch to a VTP Domain" section on page 2-18 for the procedure for verifying and resetting the VTP configuration revision number.

When you make a change to the VLAN configuration on a VTP server, the change is propagated to all switches in the VTP domain. VTP advertisements are sent over all IEEE trunk connections, including IEEE 802.1Q. VTP dynamically maps VLANs with unique names and internal index associates across multiple LAN types. Mapping eliminates excessive device administration required from network administrators.

If you configure a switch for VTP transparent mode, you can create and modify VLANs, but the changes are not sent to other switches in the domain, and they affect only the individual switch. However, configuration changes made when the switch is in this mode are saved in the switch running configuration and can be saved to the switch startup configuration file.

For domain name and password configuration guidelines, see the "Guidelines and Limitations" section on page 2-8.

VTP Modes

You can configure a supported switch to be in one of the VTP modes listed in Table 2-1.

Table 2-1 VTP Modes

VTP Mode	Description
VTP server	In VTP server mode, you can create, modify, and delete VLANs, and specify other configuration parameters (such as the VTP version) for the entire VTP domain. VTP servers advertise their VLAN configurations to other switches in the same VTP domain and synchronize their VLAN configurations with other switches based on advertisements received over trunk links. VTP server is the default mode. **Note** In VTP server mode, VLAN configurations are saved in NVRAM. If the switch detects a failure while writing a configuration to NVRAM, VTP mode automatically changes from server mode to client mode. If this happens, the switch cannot be returned to VTP server mode until the NVRAM is functioning.
VTP client	A VTP client behaves like a VTP server and transmits and receives VTP updates on its trunks, but you cannot create, change, or delete VLANs on a VTP client. VLANs are configured on another switch in the domain that is in server mode. In VTP versions 1 and 2, in VTP client mode, VLAN configurations are not saved in NVRAM. In VTP version 3, VLAN configurations are saved in NVRAM in client mode.
VTP transparent	VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2 or version 3, transparent switches do forward VTP advertisements that they receive from other switches through their trunk interfaces. You can create, modify, and delete VLANs on a switch in VTP transparent mode. In VTP versions 1 and 2, the switch must be in VTP transparent mode when you create extended-range VLANs. VTP version 3 also supports creating extended-range VLANs in client or server mode. Refer to the "Extended-Range VLANs" section on page 3-4. When the switch is in VTP transparent mode, the VTP and VLAN configurations are saved in NVRAM, but they are not advertised to other switches. In this mode, VTP mode and domain name are saved in the switch running configuration, and you can save this information in the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command.
VTP off	A switch in VTP off mode functions in the same manner as a VTP transparent switch, except that it does not forward VTP advertisements on trunks.

VTP Advertisements

Each switch in the VTP domain sends periodic global configuration advertisements from each trunk port to a reserved multicast address. Neighboring switches receive these advertisements and update their VTP and VLAN configurations as necessary.

Because trunk ports send and receive VTP advertisements, you must ensure that at least one trunk port is configured on the switch and that this trunk port is connected to the trunk port of another switch. Otherwise, the switch cannot receive any VTP advertisements. For more information on trunk ports, see Chapter 4, "Configuring VLAN Trunks."

VTP advertisements distribute this global domain information:

- VTP domain name
- VTP configuration revision number
- Update identity and update timestamp
- MD5 digest VLAN configuration, including maximum transmission unit (MTU) size for each VLAN.
- Frame format

VTP advertisements distribute this VLAN information for each configured VLAN:

- VLAN IDs (IEEE 802.1Q)
- VLAN name
- VLAN type
- VLAN state
- Additional VLAN configuration information specific to the VLAN type

In VTP version 3, VTP advertisements also include the primary server ID, an instance number, and a start index.

VTP Version 2

If you use VTP in your network, you must decide which version of VTP to use. By default, VTP operates in version 1.

VTP version 2 supports these features that are not supported in version 1:

- Token Ring support—VTP version 2 supports Token Ring Bridge Relay Function (TrBRF) and Token Ring Concentrator Relay Function (TrCRF) VLANs. For more information about Token Ring VLANs, see the "Normal-Range VLANs" section on page 3-3.
- Unrecognized Type-Length-Value (TLV) support—A VTP server or client propagates configuration changes to its other trunks, even for TLVs it is not able to parse. The unrecognized TLV is saved in NVRAM when the switch is operating in VTP server mode.
- Version-Dependent Transparent Mode—In VTP version 1, a VTP transparent switch inspects VTP messages for the domain name and version and forwards a message only if the version and domain name match. Because VTP version 2 supports only one domain, it forwards VTP messages in transparent mode without inspecting the version and domain name.

- Consistency Checks—In VTP version 2, VLAN consistency checks (such as VLAN names and values) are performed only when you enter new information through the CLI or SNMP. Consistency checks are not performed when new information is obtained from a VTP message or when information is read from NVRAM. If the MD5 digest on a received VTP message is correct, its information is accepted.

VTP Version 3

VTP version 3 supports these features that are not supported in version 1 or version 2:

- Enhanced authentication—You can configure the authentication as **hidden** or **secret**. When **hidden**, the secret key from the password string is saved in the VLAN database file, but it does not appear in plain text in the configuration. Instead, the key associated with the password is saved in hexadecimal format in the running configuration. You must reenter the password if you enter a takeover command in the domain. When you enter the **secret** keyword, you can directly configure the password secret key.
- Support for extended range VLAN (VLANs 1006 to 4094) database propagation. VTP versions 1 and 2 propagate only VLANs 1 to 1005. If extended VLANs are configured, you cannot convert from VTP version 3 to version 1 or 2.

  Note VTP pruning still applies only to VLANs 1 to 1005, and VLANs 1002 to 1005 are still reserved and cannot be modified.

- Private VLAN support.
- Support for any database in a domain. In addition to propagating VTP information, version 3 can propagate Multiple Spanning Tree (MST) protocol database information. A separate instance of the VTP protocol runs for each application that uses VTP.
- VTP primary server and VTP secondary servers. A VTP primary server updates the database information and sends updates that are honored by all devices in the system. A VTP secondary server can only back up the updated VTP configurations received from the primary server to its NVRAM.

  By default, all devices come up as secondary servers. You can enter the **vtp primary** privileged EXEC command to specify a primary server. Primary server status is only needed for database updates when the administrator issues a takeover message in the domain. You can have a working VTP domain without any primary servers. Primary server status is lost if the device reloads or domain parameters change, even when a password is configured on the switch.

- The option to turn VTP on or off on a per-trunk (per-port) basis. You can enable or disable VTP per port by entering the [**no**] **vtp** interface configuration command. When you disable VTP on trunking ports, all VTP instances for that port are disabled. You cannot set VTP to *off* for the MST database and *on* for the VLAN database on the same port.

  When you globally set VTP mode to off, it applies to all the trunking ports in the system. However, you can specify on or off on a per-VTP instance basis. For example, you can configure the switch as a VTP server for the VLAN database but with VTP *off* for the MST database.

VTP Pruning

VTP pruning increases network available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to reach the destination devices. Without VTP pruning, a switch floods broadcast, multicast, and unknown unicast traffic across all trunk links within a VTP domain even though receiving switches might discard them. VTP pruning is disabled by default.

VTP pruning blocks unneeded flooded traffic to VLANs on trunk ports that are included in the pruning-eligible list. Only VLANs included in the pruning-eligible list can be pruned. By default, VLANs 2 through 1001 are pruning eligible switch trunk ports. If the VLANs are configured as pruning-ineligible, the flooding continues. VTP pruning is supported in all VTP versions.

Figure 2-1 shows a switched network without VTP pruning enabled. Port 1 on Switch A and Port 2 on Switch D are assigned to the Red VLAN. If a broadcast is sent from the host connected to Switch A, Switch A floods the broadcast and every switch in the network receives it, even though Switches C, E, and F have no ports in the Red VLAN.

Figure 2-1 Flooding Traffic without VTP Pruning

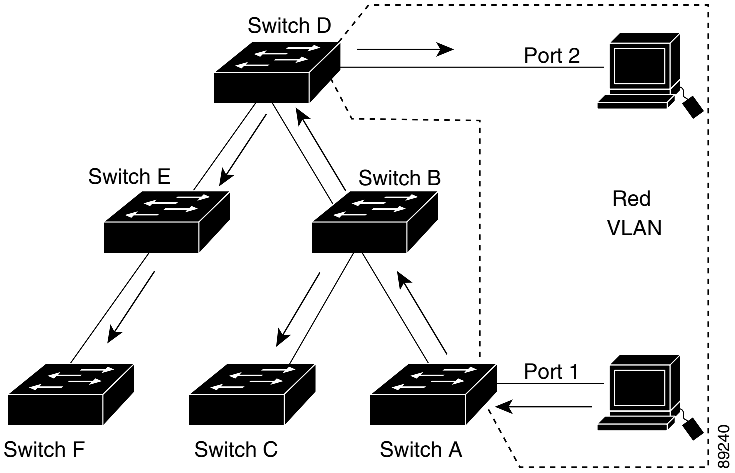
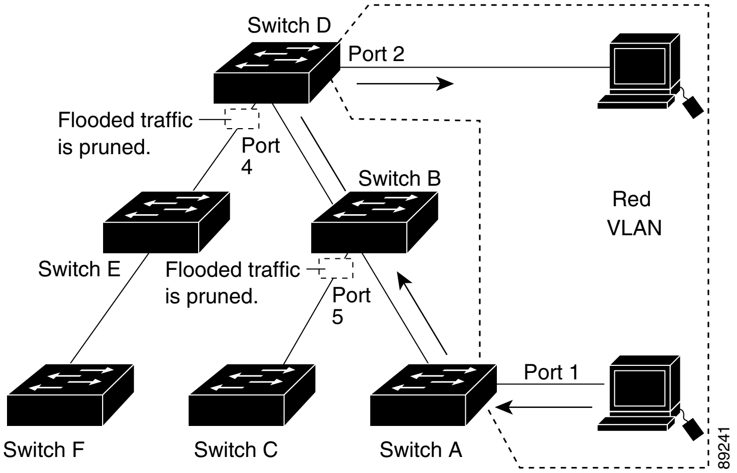


Figure 2-2 shows a switched network with VTP pruning enabled. The broadcast traffic from Switch A is not forwarded to Switches C, E, and F because traffic for the Red VLAN has been pruned on the links shown (Port 5 on Switch B and Port 4 on Switch D).

Figure 2-2 Optimized Flooded Traffic with VTP Pruning



Enabling VTP pruning on a VTP server enables pruning for the entire management domain. Making VLANs pruning-eligible or pruning-ineligible affects pruning eligibility for those VLANs on that trunk only (not on all switches in the VTP domain). (See the "Enabling VTP Pruning" section on page 2-15.)

VTP pruning takes effect several seconds after you enable it. VTP pruning does not prune traffic from VLANs that are pruning-ineligible. VLAN 1 and VLANs 1002 to 1005 are always pruning-ineligible; traffic from these VLANs cannot be pruned. Extended-range VLANs (VLAN IDs higher than 1005) are also pruning-ineligible.

VTP pruning is not designed to function in VTP transparent mode. If one or more switches in the network are in VTP transparent mode, you should do one of these:

- Turn off VTP pruning in the entire network.
- Turn off VTP pruning by making all VLANs on the trunk of the switch upstream to the VTP transparent switch pruning ineligible.

To configure VTP pruning on an interface, use the **switchport trunk pruning vlan** interface configuration command, refer to Changing the Pruning-Eligible List, page 2-16. VTP pruning operates when an interface is trunking. You can set VLAN pruning-eligibility, whether or not VTP pruning is enabled for the VTP domain, whether or not any given VLAN exists, and whether or not the interface is currently trunking.

Prerequisites

- Ensure that at least one trunk port is configured on the switch and that this trunk port is connected to the trunk port of another switch. (See Chapter 4, "Configuring VLAN Trunks.")
- If you use VTP in your network, you must decide which version of VTP to use. By default, VTP operates in version 1.

Guidelines and Limitations

You use the **vtp** global configuration command to set the VTP password, the version, the VTP file name, the interface providing updated VTP information, the domain name, and the mode, and to disable or enable pruning. For more information about available keywords, see the command descriptions in the *Cisco IOS LAN Switching Command Reference*. The VTP information is saved in the VTP VLAN database. When VTP mode is transparent, the VTP domain name and mode are also saved in the switch running configuration file, and you can save it in the switch startup configuration file by entering the **copy running-config startup-config** privileged EXEC command. You must use this command if you want to save VTP mode as transparent if the switch resets.

When you save VTP information in the switch startup configuration file and restart the switch, the configuration is selected as follows:

- If the VTP mode is transparent in both the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared). The VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or the domain name in the startup configuration does not match the VLAN database, the domain name and the VTP mode and configuration for the first 255 VLANs use the VLAN database information.

Domain Names

When configuring VTP for the first time, you must always assign a domain name. You must configure all switches in the VTP domain with the same domain name. Switches in VTP transparent mode do not exchange VTP messages with other switches, and you do not need to configure a VTP domain name for them.

Note If NVRAM and DRAM storage is sufficient, all switches in a VTP domain should be in VTP server mode.

Caution Do not configure a VTP domain if all switches are operating in VTP client mode. If you configure the domain, it is impossible to make changes to the VLAN configuration of that domain. Make sure that you configure at least one switch in the VTP domain for VTP server mode.

Passwords

You can configure a password for the VTP domain, but it is not required. If you do configure a domain password, all domain switches must share the same password and you must configure the password on each switch in the management domain. Switches without a password or with the wrong password reject VTP advertisements.

If you configure a VTP password for a domain, a switch that is booted without a VTP configuration does not accept VTP advertisements until you configure it with the correct password. After the configuration, the switch accepts the next VTP advertisement that uses the same password and domain name in the advertisement.

If you are adding a new switch to an existing network with VTP capability, the new switch learns the domain name only after the applicable password has been configured on it.

Caution When you configure a VTP domain password, the management domain does not function properly if you do not assign a management domain password to each switch in the domain.

VTP Version

Follow these guidelines when deciding which VTP version to implement:

- All switches in a VTP domain must have the same domain name, but they do not need to run the same VTP version.
- A VTP version 2-capable switch can operate in the same VTP domain as a switch running VTP version 1 if version 2 is disabled on the version 2-capable switch (version 2 is disabled by default).
- If a switch running VTP version 1 but capable of running VTP version 2 receives VTP version 3 advertisements, it automatically moves to VTP version 2.
- If a switch running VTP version 3 is connected to a switch running VTP version 1, the VTP version 1 switch moves to VTP version 2, and the VTP version 3 switch sends scaled-down versions of the VTP packets so that the VTP version 2 switch can update its database.
- A switch running VTP version 3 cannot move to version 1 or 2 if it has extended VLANs.
- Do not enable VTP version 2 on a switch unless all of the switches in the same VTP domain are version-2-capable. When you enable version 2 on a switch, all of the version-2-capable switches in the domain enable version 2. If there is a version 1-only switch, it does not exchange VTP information with switches that have version 2 enabled.
- We recommend placing VTP version 1 and 2 switches at the edge of the network because they do not forward VTP version 3 advertisements.
- If there are TrBRF and TrCRF Token Ring networks in your environment, you must enable VTP version 2 or version 3 for Token Ring VLAN switching to function properly. To run Token Ring and Token Ring-Net, disable VTP version 2.
- VTP version 1 and version 2 do not propagate configuration information for extended-range VLANs (VLANs 1006 to 4094). You must configure these VLANs manually on each device. VTP version 3 supports extended-range VLANs. You cannot convert from VTP version 3 to VTP version 2 if extended VLANs are configured.
- When a VTP version 3 device trunk port receives messages from a VTP version 2 device, it sends a scaled-down version of the VLAN database on that particular trunk in VTP version 2 format. A VTP version 3 device does not send VTP version 2-formatted packets on a trunk unless it first receives VTP version 2 packets on that trunk port.
- When a VTP version 3 device detects a VTP version 2 device on a trunk port, it continues to send VTP version 3 packets, in addition to VTP version 2 packets, to allow both kinds of neighbors to coexist on the same trunk.
- A VTP version 3 device does not accept configuration information from a VTP version 2 or version 1 device.
- Two VTP version 3 regions can only communicate in transparent mode over a VTP version 1 or version 2 region.
- Devices that are only VTP version 1 capable cannot interoperate with VTP version 3 devices.

Configuration Requirements

If you are configuring VTP on a cluster member switch to a VLAN, use the **rcommand** privileged EXEC command to log in to the member switch. For more information about the command, see the command reference for this release.

In VTP versions 1 and 2, when you configure extended-range VLANs on the switch, the switch must be in VTP transparent mode. VTP version 3 also supports creating extended-range VLANs in client or server mode.

Default Settings

Feature	Default Setting
VTP domain name	Null.
VTP mode (VTP version 1 and version 2)	Server.
VTP mode (VTP version 3)	The mode is the same as the mode in VTP version 1 or 2 before conversion to version 3.
VTP version	Version 1.
MST database mode	Transparent.
VTP version 3 server type	Secondary.
VTP password	None.
VTP pruning	Disabled.

Configuring VTP

This section includes the following topics:

- Configuring VTP Mode, page 2-10
- Enabling the VTP Version, page 2-14
- Enabling VTP Pruning, page 2-15
- Changing the Pruning-Eligible List, page 2-16
- Configuring VTP on a Per-Port Basis, page 2-18
- Adding a VTP Client Switch to a VTP Domain, page 2-18

Configuring VTP Mode

You can configure VTP mode as one of these:

- When a switch is in VTP server mode, you can change the VLAN configuration and have it propagated throughout the network.
- When a switch is in VTP client mode, you cannot change its VLAN configuration. The client switch receives VTP updates from a VTP server in the VTP domain and then modifies its configuration accordingly.
- When you configure the switch for VTP transparent mode, VTP is disabled on the switch. The switch does not send VTP updates and does not act on VTP updates received from other switches. However, a VTP transparent switch running VTP version 2 does forward received VTP advertisements on its trunk links.

- VTP off mode is the same as VTP transparent mode except that VTP advertisements are not forwarded.

BEFORE YOU BEGIN

Follow these guidelines:

- For VTP version 1 and version 2, if extended-range VLANs are configured on the switch, you cannot change VTP mode to client or server. You receive an error message, and the configuration is not allowed. VTP version 1 and version 2 do not propagate configuration information for extended range VLANs (VLANs 1006 to 4094). You must manually configure these VLANs on each device.

Note For VTP version 1 and 2, before you create extended-range VLANs (VLAN IDs 1006 to 4094), you must set VTP mode to transparent by using the **vtp mode transparent** global configuration command. Save this configuration to the startup configuration so that the switch starts in VTP transparent mode. Otherwise, you lose the extended-range VLAN configuration if the switch resets and boots up in VTP server mode (the default).

- VTP version 3 supports extended-range VLANs. If extended VLANs are configured, you cannot convert from VTP version 3 to VTP version 2.
- If you configure the switch for VTP client mode, the switch does not create the VLAN database file (vlan.dat). If the switch is then powered off, it resets the VTP configuration to the default. To keep the VTP configuration with VTP client mode after the switch restarts, you must first configure the VTP domain name before the VTP mode.

Caution If all switches are operating in VTP client mode, do not configure a VTP domain name. If you do, it is impossible to make changes to the VLAN configuration of that domain. Therefore, make sure you configure at least one switch as a VTP server.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vtp domain** *domain-name*	Configure the VTP administrative-domain name. The name can be 1 to 32 characters. All switches operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name. This command is optional for modes other than server mode. VTP server mode requires a domain name. If the switch has a trunk connection to a VTP domain, the switch learns the domain name from the VTP server in the domain. You should configure the VTP domain before configuring other VTP parameters.

	Command	Purpose
Step 3	**vtp mode** {**client** | **server** | **transparent** | **off**} {**vlan** | **mst** | **unknown**}	Configure the switch for VTP mode (client, server, transparent or off). (Optional) Configure the database: • **vlan**—the VLAN database is the default if none are configured. • **mst**—the multiple spanning tree (MST) database. • **unknown**—an unknown database type.
Step 4	**vtp password** *password*	(Optional) Set the password for the VTP domain. The password can be 8 to 64 characters. If you configure a VTP password, the VTP domain does not function properly if you do not assign the same password to each switch in the domain. See the "Configuring a VTP Version 3 Password" section on page 2-12 for options available with VTP version 3.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show vtp status**	Verify your entries in the *VTP Operating Mode* and the *VTP Domain Name* fields of the display.
Step 7	**copy running-config startup-config**	(Optional) Save the configuration in the startup configuration file. **Note** Only VTP mode and domain name are saved in the switch running configuration and can be copied to the startup configuration file.

When you configure a domain name, it cannot be removed; you can only reassign a switch to a different domain.

To return a switch in another mode to VTP server mode, use the **no vtp mode** global configuration command. To return the switch to a no-password state, use the **no vtp password** global configuration command.

EXAMPLE

This example shows how to configure the switch as a VTP server with the domain name *eng_group* and the password *mypassword*:

```
Switch(config)# vtp domain eng_group
Setting VTP domain name to eng_group.
Switch(config)# vtp mode server
Setting device to VTP Server mode for VLANS.
Switch(config)# vtp password mypassword
Setting device VLAN database password to mypassword.
Switch(config)# end
```

Configuring a VTP Version 3 Password

BEFORE YOU BEGIN

- Configure the VTP domain and VTP mode as described in the "Configuring VTP Mode" procedure on page 2-10.
- Follow this procedure for VTP version 3 only.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vtp password** *password* [**hidden** | **secret**]	(Optional) Set the password for the VTP domain. The password can be 8 to 64 characters. • (Optional) **hidden**—Enter **hidden** to ensure that the secret key generated from the password string is saved in the nvam:vlan.dat file. If you configure a takeover by configuring a VTP primary server, you are prompted to reenter the password. • (Optional) **secret**—Enter **secret** to directly configure the password. The secret password must contain 32 hexadecimal characters.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vtp password**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save the configuration in the startup configuration file.

To clear the password, enter the **no vtp password** global configuration command.

EXAMPLE

This example shows how to configure a hidden password and how it appears:

```
Switch(config)# vtp password mypassword hidden
Generating the secret associated to the password.
Switch(config)# end
Switch# show vtp password
VTP password: 89914640C8D90868B6A0D8103847A733
```

Configuring a VTP Version 3 Primary Server

Follow this procedure to configure a VTP version 3 server as a VTP primary server, which starts a takeover operation.

BEFORE YOU BEGIN

- Configure the VTP domain and VTP mode as described in the "Configuring VTP Mode" procedure on page 2-10.
- Follow this procedure for VTP version 3 only.

DETAILED STEPS

	Command	Purpose
Step 1	**vtp primary-server** [**vlan** | **mst**] [**force**]	Change the operational state of a switch from a secondary server (the default) to a primary server and advertise the configuration to the domain. If the switch password is configured as **hidden**, you are prompted to reenter the password. • (Optional) **vlan**—Select the VLAN database as the takeover feature. This is the default. • (Optional) **mst**—Select the multiple spanning tree (MST) database as the takeover feature. • (Optional) **force**—Entering **force** overwrites the configuration of any conflicting servers. If you do not enter **force**, you are prompted for confirmation before the takeover.

EXAMPLE

This example shows how to configure a switch as the primary server for the VLAN database (the default) when a hidden or secret password was configured:

```
Switch# vtp primary vlan
Enter VTP password: mypassword
This switch is becoming Primary server for vlan feature in the VTP  domain

VTP Database Conf Switch ID      Primary Server Revision System Name
------------ ---- -------------- -------------- -------- --------------------
VLANDB       Yes  00d0.00b8.1400=00d0.00b8.1400 1        stp7

Do you want to continue (y/n) [n]? y
```

Enabling the VTP Version

VTP version 2 and version 3 are disabled by default.

BEFORE YOU BEGIN

- When you enable VTP version 2 on a switch, every VTP version 2-capable switch in the VTP domain enables version 2. To enable VTP version 3, you must manually configure it on each switch.
- With VTP versions 1 and 2, you can configure the version only on switches in VTP server or transparent mode. If a switch is running VTP version 3, you can change to version 2 when the switch is in client mode if no extended VLANs exist, no private VLANs exist, and no hidden password was configured.

Caution VTP version 1 and VTP version 2 are not interoperable on switches in the same VTP domain. Do not enable VTP version 2 unless every switch in the VTP domain supports version 2.

- In TrCRF and TrBRF Token ring environments, you must enable VTP version 2 or VTP version 3 for Token Ring VLAN switching to function properly. For Token Ring and Token Ring-Net media, disable VTP version 2 must be disabled.

- VTP version 3 is supported on switches running Cisco IOS Release 12.2(52) SE or later.

Caution In VTP version 3, both the primary and secondary servers can exist on an instance in the domain.

For more information on VTP version configuration guidelines, see the "VTP Version" section on page 2-9.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vtp version** {**1** | **2** | **3**}	Enable the VTP version on the switch. The default is VTP version 1.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vtp status**	Verify that the configured VTP version is enabled.
Step 5	**copy running-config startup-config**	(Optional) Save the configuration in the startup configuration file.

To return to the default VTP version 1, use the **no vtp version** global configuration command**.**

EXAMPLE

```
Switch(config)# vtp version 3
Switch(config)# end
```

Enabling VTP Pruning

Pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the destination devices. You can only enable VTP pruning on a switch in VTP server mode.

With VTP versions 1 and 2, when you enable pruning on the VTP server, it is enabled for the entire VTP domain. In VTP version 3, you must manually enable pruning on each switch in the domain.

Only VLANs included in the pruning-eligible list can be pruned. By default, VLANs 2 through 1001 are pruning-eligible on trunk ports. Reserved VLANs and extended-range VLANs cannot be pruned. To change the pruning-eligible VLANs, see the "Changing the Pruning-Eligible List" section on page 2-16.

BEFORE YOU BEGIN

Configure the switch for VTP server mode as described in "Configuring VTP Mode" procedure on page 2-10.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vtp pruning**	Enable pruning in the VTP administrative domain. By default, pruning is disabled. You need to enable pruning on only one switch in VTP server mode.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vtp status**	Verify your entries in the *VTP Pruning Mode* field of the display.

To disable VTP pruning, use the **no vtp pruning** global configuration command.

EXAMPLE

This example shows how to enable VTP pruning and check the VTP pruning status:

```
Switch(config)# vtp pruning
Switch(config)# end
Switch# show vtp status
VTP Version capable               : 1 to 3
VTP version running               : 2
VTP Domain Name                   : cisco
VTP Pruning Mode                  : Enabled
VTP Traps Generation              : Disabled
Device ID                         : 0012.44dc.b800
MD5 digest                        : 0x61 0x98 0xD0 0xAD 0xA4 0x8C 0x53 0x35
Configuration last modified by 10.10.0.0 at 8-7-12 06:56:27
Local updater ID is 10.10.0.0 on interface Lo0 (first layer3 interface found)
Feature VLAN:
--------------
VTP Mode                             : Server
Maximum VLANs supported locally      : 1005
Number if existing VLANs             : 53
Revision                             : 1
Switch#
```

Changing the Pruning-Eligible List

The pruning-eligible list applies only to trunk ports. Each trunk port has its own eligibility list. Follow this procedure to remove VLANs from the pruning-eligible list on a trunk port. VTP pruning must be enabled for this procedure to take effect.

BEFORE YOU BEGIN

Enable VTP pruning as described in the “Enabling VTP Pruning” procedure on page 2-15.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Identify an interface, and enter interface configuration mode.
Step 3	**switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**} *vlan-list* [,*vlan*[,*vlan*[,,,]]	Configure the list of VLANs allowed to be pruned from the trunk. (See the "Enabling VTP Pruning" section on page 2-15.) **add**—Adds the defined list of VLANs to those currently set, instead of replacing the list. **except**—Lists the VLANs that should be calculated by inverting the defined list of VLANs. **none**—Indicates an empty list. **remove**—Removes the defined list of VLANs from those currently set instead of replacing the list. *vlan-list*—Is either a single VLAN number from 1 to 1005 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen that represents the VLAN IDs of the allowed VLANs when this port is in trunking mode. For explanations about using the add, except, none, and remove keywords, refer to the *Cisco IOS Interface and Hardware Component Command Reference*. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Valid IDs are from 2 to 1001. VLANs that are pruning-ineligible receive flooded traffic. The default list of VLANs allowed to be pruned contains VLANs 2 to 1001. **Note** To return to the default pruning-eligible list of all VLANs, use the **no switchport trunk pruning vlan** interface configuration command.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Pruning VLANs Enabled* field of the command display.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to remove VLANs 3 and 10 to 15 from the pruning-eligible list:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport trunk pruning vlan remove 3,10-15
```

Configuring VTP on a Per-Port Basis

With VTP version 3, you can enable or disable VTP on a per-port basis. You can enable VTP only on ports that are in trunk mode. Incoming and outgoing VTP traffic are blocked, not forwarded.

BEFORE YOU BEGIN

Ensure that the switch is running VTP version 3 as described in the "Enabling the VTP Version" procedure on page 2-14 and that the port is a trunk port. (See the "Configuring a Trunk Port" section on page 4-4.)

DETAILED STEPS

Beginning in privileged EXEC mode, follow these steps to enable VTP on a port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Identify an interface, and enter interface configuration mode.
Step 3	**vtp**	Enable VTP on the specified port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config interface** *interface-id*	Verify the change to the port.
Step 6	**show vtp status**	Verify the configuration.

To disable VTP on the interface, use the **no vtp** interface configuration command.

EXAMPLE

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# vtp
Switch(config-if)# end
```

Adding a VTP Client Switch to a VTP Domain

Before adding a VTP client to a VTP domain, always verify that its VTP configuration revision number is *lower* than the configuration revision number of the other switches in the VTP domain. Switches in a VTP domain always use the VLAN configuration of the switch with the highest VTP configuration revision number. With VTP versions 1 and 2, adding a switch that has a revision number higher than the revision number in the VTP domain can erase all VLAN information from the VTP server and VTP domain. With VTP version 3, the VLAN information is not erased.

Follow this procedure to verify and reset the VTP configuration revision number on a switch *before* adding it to a VTP domain.

BEFORE YOU BEGIN

Configure the VTP domain and VTP mode as described in the "Configuring VTP Mode" procedure on page 2-10.

DETAILED STEPS

	Command	Purpose
Step 1	**show vtp status**	Check the VTP configuration revision number. If the number is 0, add the switch to the VTP domain. If the number is greater than 0, follow these steps: **a.** Write down the domain name. **b.** Write down the configuration revision number. **c.** Continue with the next steps to reset the switch configuration revision number.
Step 2	**configure terminal**	Enter global configuration mode.
Step 3	**vtp domain** *domain-name*	Change the domain name from the original one displayed in Step 1 to a new name.
Step 4	**end**	The VLAN information on the switch is updated and the configuration revision number is reset to 0. You return to privileged EXEC mode.
Step 5	**show vtp status**	Verify that the configuration revision number has been reset to 0.
Step 6	**configure terminal**	Enter global configuration mode.
Step 7	**vtp domain** *domain-name*	Enter the original domain name on the switch.
Step 8	**end**	The VLAN information on the switch is updated, and you return to privileged EXEC mode.
Step 9	**show vtp status**	(Optional) Verify that the domain name is the same as in Step 1 and that the configuration revision number is 0.

After resetting the configuration revision number, add the switch to the VTP domain.

Note You can use the **vtp mode transparent** global configuration command to disable VTP on the switch and then to change its VLAN information without affecting the other switches in the VTP domain.

EXAMPLE

This example shows how to reset the configuration revision number of the switch to 0:

```
Switch# show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0012.44dc.b800
MD5 digest                      : 0x61 0x98 0xD0 0xAD 0xA4 0x8C 0x53 0x35
Configuration last modified by 10.10.0.0 at 5-9-13 06:56:27
Local updater ID is 10.10.0.0 on interface Lo0 (first layer3 interface found)
Feature VLAN:
--------------
VTP Mode                           : Server
Maximum VLANs supported locally    : 1005
Number if existing VLANs           : 53
Revision                           : 1
```

```
Switch# configure terminal
Switch(config)# vtp domain test
Switch(config)# end
Switch# show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : test
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0012.44dc.b800
MD5 digest                      : 0x61 0x98 0xD0 0xAD 0xA4 0x8C 0x53 0x35
Configuration last modified by 10.10.0.0 at 5-9-13 06:58:43
Local updater ID is 10.10.0.0 on interface Lo0 (first layer3 interface found)
Feature VLAN:
--------------
VTP Mode                           : Server
Maximum VLANs supported locally    : 1005
Number if existing VLANs           : 53
Revision                           : 0
Switch# configure terminal
Switch(config)# vtp domain cisco
Switch(config)# end
```

Verifying Configuration

Command	Purpose
show vtp counters	Display counters about VTP messages that have been sent and received.
show vtp devices [**conflict**]	Display information about all VTP version 3 devices in the domain. Conflicts are VTP version 3 devices with conflicting primary servers. The **show vtp devices** command does not display information when the switch is in transparent or off mode.
show vtp interface [*interface-id*]	Display VTP status and configuration for all interfaces or the specified interface.
show vtp password	Display the VTP password. The form of the password displayed depends on whether or not the **hidden** keyword was entered and if encryption is enabled on the switch.
show vtp status	Display the VTP switch configuration information.

Configuration Example

This example shows how to configure the switch as a VTP server with the domain name *eng_group* and the password *mypassword*:

```
Switch(config)# vtp domain eng_group
Setting VTP domain name to eng_group.
Switch(config)# vtp mode server
Setting device to VTP Server mode for VLANS.
Switch(config)# vtp password mypassword
Setting device VLAN database password to mypassword.
Switch(config)# end
```

This example shows how to configure a hidden password and how it appears:

```
Switch(config)# vtp password mypassword hidden
Generating the secret associated to the password.
Switch(config)# end
Switch# show vtp password
VTP password: 89914640C8D90868B6A0D8103847A733
```

This example shows how to configure a switch as the primary server for the VLAN database (the default) when a hidden or secret password was configured:

```
Switch# vtp primary vlan
Enter VTP password: mypassword
This switch is becoming Primary server for vlan feature in the VTP  domain

VTP Database Conf Switch ID      Primary Server Revision System Name
------------ ---- -------------- -------------- -------- --------------------
VLANDB       Yes  00d0.00b8.1400=00d0.00b8.1400 1        stp7

Do you want to continue (y/n)  [n]? y
```

This example shows how to enable VTP version 3:

```
Switch(config)# vtp version 3
Switch(config)# end
```

This example shows how to enable VTP pruning and check the VTP pruning status:

```
Switch(config)# vtp pruning
Switch(config)# end
Switch# show vtp status
VTP Version capable              : 1 to 3
VTP version running              : 2
VTP Domain Name                  : cisco
VTP Pruning Mode                 : Enabled
VTP Traps Generation             : Disabled
Device ID                        : 0012.44dc.b800
MD5 digest                       : 0x61 0x98 0xD0 0xAD 0xA4 0x8C 0x53 0x35
Configuration last modified by 10.10.0.0 at 8-7-12 06:56:27
Local updater ID is 10.10.0.0 on interface Lo0 (first layer3 interface found)
Feature VLAN:
--------------
VTP Mode                            : Server
Maximum VLANs supported locally     : 1005
Number if existing VLANs            : 53
Revision                            : 1
Switch#
```

This example shows how to remove VLANs 3 and 10 to 15 from the pruning-eligible list:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport trunk pruning vlan remove 3,10-15
```

This example shows how to enable VTP on an interface:

```
Switch(config-if)# vtp
Switch(config-if)# end
```

This example shows how to reset the configuration revision number of the switch to 0:

```
Switch# show vtp status
VTP Version capable              : 1 to 3
VTP version running              : 2
VTP Domain Name                  : cisco
VTP Pruning Mode                 : Disabled
VTP Traps Generation             : Disabled
```

```
Device ID                          : 0012.44dc.b800
MD5 digest                         : 0x61 0x98 0xD0 0xAD 0xA4 0x8C 0x53 0x35
Configuration last modified by 10.10.0.0 at 5-9-13 06:56:27
Local updater ID is 10.10.0.0 on interface Lo0 (first layer3 interface found)
Feature VLAN:
--------------
VTP Mode                              : Server
Maximum VLANs supported locally       : 1005
Number if existing VLANs              : 53
Revision                              : 1
Switch# configure terminal
Switch(config)# vtp domain test
Switch(config)# end
Switch# show vtp status

VTP Version capable                : 1 to 3
VTP version running                : 2
VTP Domain Name                    : test
VTP Pruning Mode                   : Disabled
VTP Traps Generation               : Disabled
Device ID                          : 0012.44dc.b800
MD5 digest                         : 0x61 0x98 0xD0 0xAD 0xA4 0x8C 0x53 0x35
Configuration last modified by 10.10.0.0 at 5-9-13 06:58:43
Local updater ID is 10.10.0.0 on interface Lo0 (first layer3 interface found)
Feature VLAN:
--------------
VTP Mode                              : Server
Maximum VLANs supported locally       : 1005
Number if existing VLANs              : 53
Revision                              : 0
Switch# configure terminal
Switch(config)# vtp domain cisco
Switch(config)# end
```

Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS LAN Switching Command Reference
- Cisco IOS Interface and Hardware Component Command Reference

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520 Switch	Cisco IOS Release 15.0(2)ED
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 15.0(2)ED

CHAPTER 3

Configuring VLANs

This chapter describes how to configure normal-range VLANs (VLAN IDs 1 to 1005) and extended-range VLANs (VLAN IDs 1006 to 4094) on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*. It includes information about VLAN membership modes, VLAN configuration modes, VLAN trunks, and dynamic VLAN assignment from a VLAN Membership Policy Server (VMPS).

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 3-16.

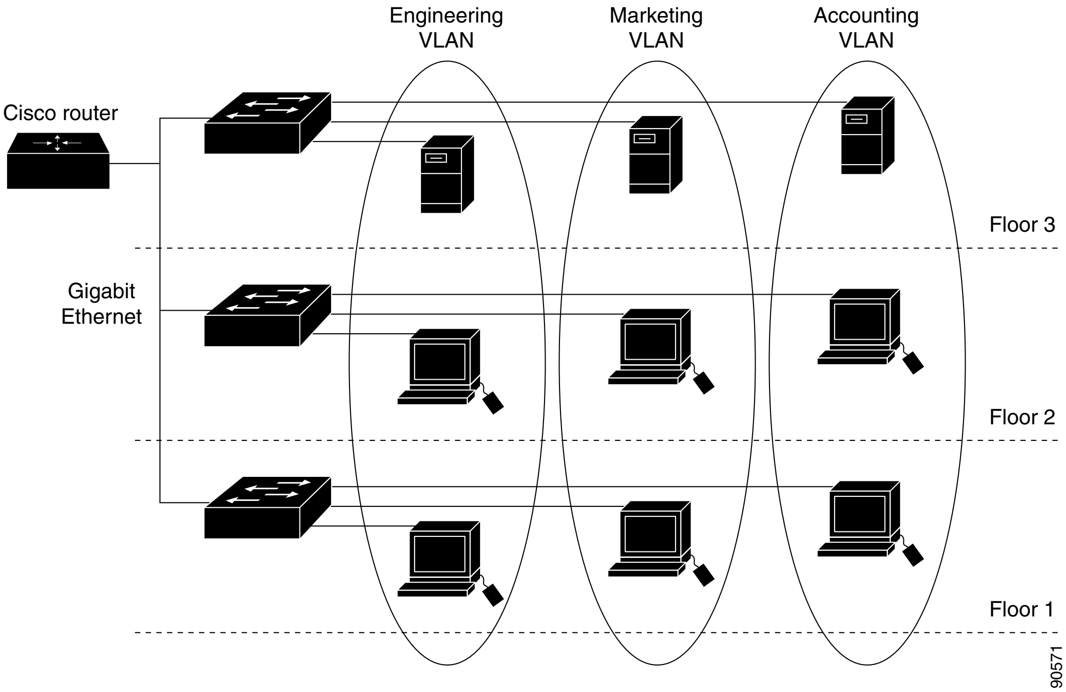
This chapter includes the following sections:

Information About VLANs

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router, as shown in Figure 3-1. Because a VLAN is considered a separate logical network, it contains its own bridge MIB information and can support its own implementation of spanning tree. (See Chapter 11, "Configuring STP.")

Figure 3-1 shows an example of VLANs segmented into logically defined networks.

Figure 3-1 VLANs as Logically Defined Networks



VLANs are often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the switch is assigned manually on an interface-by-interface basis. When you assign switch interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

Traffic between VLANs must be routed. Switches that are running the IP services image can route traffic between VLANs by using switch virtual interfaces (SVIs). To route traffic between VLANs, an SVI must be explicitly configured and assigned an IP address. For more information, see the “Switch Virtual Interfaces” section and the “Configuring Layer 3 Interfaces” section in the *Interfaces Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.

This section includes the following topics:

- Supported VLANs, page 3-2
- Normal-Range VLANs, page 3-3
- Extended-Range VLANs, page 3-4
- VLAN Port Membership Modes, page 3-4
- UNI-ENI VLANs, page 3-5

Supported VLANs

VLANs are identified with a number from 1 to 4094. VLAN IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs. VLAN IDs greater than 1005 are extended-range VLANs and are not stored in the VLAN database.

Although the switch supports a total of 1005 (normal-range and extended-range) VLANs, the number of routed ports, SVIs, and other configured features affects the use of the switch hardware.

The switch supports per-VLAN spanning-tree plus (PVST+) or rapid PVST+ with a maximum of 128 spanning-tree instances. One spanning-tree instance is allowed per VLAN.

Note Network node interfaces (NNIs) support STP by default. Enhanced network interfaces (ENIs) can be configured to support STP. User network interfaces (UNIs) do not support STP and by default are always in a forwarding state.

See the "Guidelines and Limitations" section on page 3-7 for more information about the number of spanning-tree instances and the number of VLANs. The switch supports IEEE 802.1Q trunking for sending VLAN traffic over Ethernet ports.

Normal-Range VLANs

Normal-range VLANs are VLANs with VLAN IDs 1 to 1005. You can add, modify or remove configurations for VLANs 2 to 1001 in the VLAN database. (VLAN IDs 1 and 1002 to 1005 are automatically created and cannot be removed.)

Configurations for VLAN IDs 1 to 1005 are written to the file *vlan.dat* (VLAN database), and you can display them by entering the **show vlan** privileged EXEC command. The *vlan.dat* file is stored in flash memory.

Caution You can cause inconsistency in the VLAN database if you try to manually delete the *vlan.dat* file. If you want to modify the VLAN configuration, use the commands described in these sections and in the command reference for this release.

You can set these parameters when you create a new normal-range VLAN or modify an existing VLAN in the VLAN database:

- VLAN ID
- VLAN name
- VLAN type (Ethernet, Fiber Distributed Data Interface [FDDI], FDDI network entity title [NET], TrBRF, or TrCRF, Token Ring, Token Ring-Net)

  Note The switch supports only Ethernet VLANs. You can configure parameters for FDDI and Token Ring VLANs and view the results in the vlan.dat file, but these parameters are not used.

- VLAN state (active or suspended)
- Maximum transmission unit (MTU) for the VLAN
- Security Association Identifier (SAID)
- Bridge identification number for TrBRF VLANs
- Ring number for FDDI and TrCRF VLANs
- Parent VLAN number for TrCRF VLANs
- Spanning Tree Protocol (STP) type for TrCRF VLANs

- VLAN number to use when translating from one VLAN type to another
- Private VLAN. Configure the VLAN as a primary or secondary private VLAN. For information about private VLANs, see Chapter 7, "Configuring Private VLANs."
- Remote SPAN VLAN. Configure the VLAN as the Remote Switched Port Analyzer (RSPAN) VLAN for a remote SPAN session. For more information on remote SPAN, see the "Configuring SPAN and RSPAN" chapter in the *System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.
- UNI-ENI VLAN configuration

For extended-range VLANs, you can configure only MTU, private VLAN, remote SPAN VLAN, and UNI-ENI VLAN parameters.

Note This chapter does not provide configuration details for most of these parameters. For complete information on the commands and parameters that control VLAN configuration, see the documents listed in the "Related Documents" section on page 3-16.

Extended-Range VLANs

You can create extended-range VLANs (in the range 1006 to 4094) to enable service providers to extend their infrastructure to a greater number of customers. The extended-range VLAN IDs are allowed for any **switchport** commands that allow VLAN IDs. Extended-range VLAN configurations are not stored in the VLAN database, but they are stored in the switch running configuration file, and you can save the configuration in the startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

Note Although the switch supports 4094 VLAN IDs, the actual number of VLANs supported is 1005.

VLAN Port Membership Modes

You configure a port to belong to a VLAN by assigning a membership mode that specifies the kind of traffic that the port carries and the number of VLANs to which it can belong. Table 3-1 lists the membership modes and characteristics.

Table 3-1 Port Membership Modes

Membership Mode	VLAN Membership Characteristics
Static-access	A static-access port can belong to one VLAN and is manually assigned to that VLAN. For more information, see the "Assigning Static-Access Ports to a VLAN" section on page 3-11.
Trunk (802.1Q)	A trunk port is a member of all VLANs by default, including extended-range VLANs, but membership can be limited by configuring the allowed-VLAN list. For information about configuring trunk ports, see the "Configuring VLAN Trunks" section on page 4-3.

Table 3-1 Port Membership Modes

Membership Mode	VLAN Membership Characteristics
Dynamic-access	A dynamic-access port can belong to one VLAN (VLAN ID 1 to 4094) and is dynamically assigned by a VLAN Membership Policy Server (VMPS). The VMPS can be a Catalyst 5000 or Catalyst 6500 series switch, for example, but never a Cisco Connected Grid switch. The Cisco Connected Grid switch is a VMPS client. See Chapter 6, "Configuring VMPS." **Note** Only UNIs or ENIs can be dynamic-access ports. You can have dynamic-access ports and trunk ports on the same switch, but you must connect the dynamic-access port to an end station or hub and not to another switch. For configuration information, see the "Configuring Dynamic-Access Ports on VMPS Clients" section on page 6-57.
Private VLAN	A private VLAN port is a host or promiscuous port that belongs to a primary or secondary private VLAN. Only NNIs can be configured as promiscuous ports. For information about private VLANs, see Chapter 7, "Configuring Private VLANs."
Tunnel (**dot1q-tunnel**)	Tunnel ports are used for 802.1Q tunneling to maintain customer VLAN integrity across a service-provider network. You configure a tunnel port on an edge switch in the service-provider network and connect it to an 802.1Q trunk port on a customer interface, creating an assymetric link. A tunnel port belongs to a single VLAN that is dedicated to tunneling. For more information about tunnel ports, see Chapter 10, "Configuring Layer 2 Protocol Tunneling."

For more detailed definitions of access and trunk modes and their functions, see Table 4-1 in Chapter 4, "Configuring VLAN Trunks."

When a port belongs to a VLAN, the switch learns and manages the addresses associated with the port on a per-VLAN basis. For more information, see the "Managing the MAC Address Table" section of the "Administering the Switch" chapter in the *System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.

UNI-ENI VLANs

The switch is the boundary between customer networks and the service-provider network, with user network interfaces (UNIs) and enhanced network interfaces (ENIs) connected to the customer side of the network. When customer traffic enters or leaves the service-provider network, the customer VLAN ID must be isolated from other customers' VLAN IDs. You can achieve this isolation by several methods, including using private VLANs. On the switch, this isolation occurs by default by using UNI-ENI VLANs.

There are two types of UNI-ENI VLANs:

- UNI-ENI isolated VLAN—This is the default VLAN state for all VLANs created on the switch. Local switching does not occur among UNIs or ENIs on the switch that belong to the same UNI-ENI isolated VLAN. This configuration is designed for cases when different customers are connected to UNIs or ENIs on the same switch. However, switching is allowed among UNIs or ENIs on different switches even though they belong to the same UNI-ENI isolated VLAN.
- UNI-ENI community VLAN—Local switching is allowed among UNIs and ENIs on the switch that belong to the same community VLAN. If UNIs or ENIs belong to the same customer, and you want to switch packets between the ports, you can configure the common VLAN as a UNI-ENI

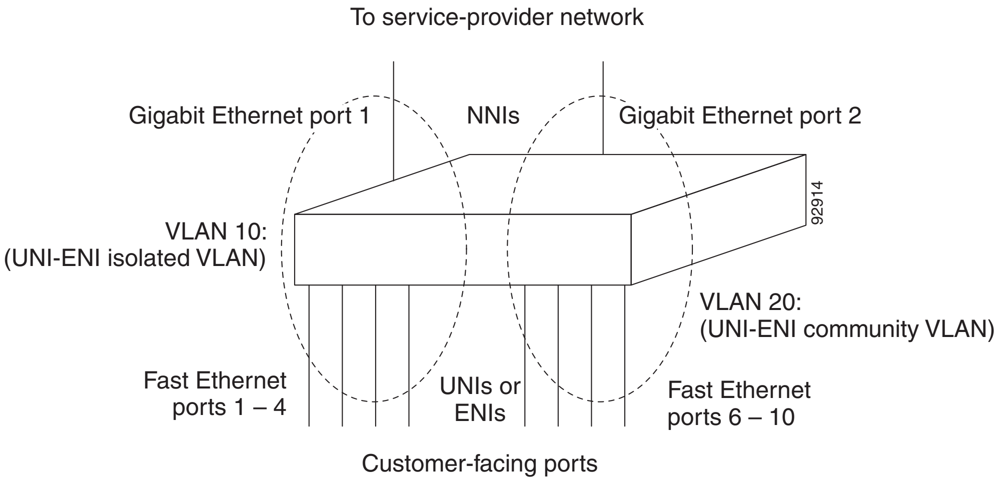
community VLAN. There is no local switching between the ports in a UNI-ENI community VLAN and ports outside of the VLAN. The switch supports a combination of only eight UNIs and ENIs in a UNI-ENI community VLAN.

Note Local switching takes place between ENIs and UNIs in the same community VLAN. Because you can enable spanning tree on ENIs, but not on UNIs, you should use caution when configuring ENIs and UNIs in the same community VLAN. UNIs are always in the forwarding state.

Network node interfaces (NNIs) are not affected by the type of UNI-ENI VLAN to which they belong. Switching can occur between NNIs and other NNIs or UNIs or ENIs on the switch or other switches that are part of the same VLAN, regardless of VLAN type.

In the configuration in Figure 3-2, if VLAN 10 is a UNI-ENI isolated VLAN and VLAN 20 is a UNI-ENI community VLAN, local switching does not take place among Fast Ethernet ports 1–4, but local switching can occur between Fast Ethernet ports 6–10. The NNIs in both VLAN 10 and VLAN 20 can exchange packets with the UNIs or ENIs in the same VLAN.

Figure 3-2 UNI-ENI Isolated and Community VLANs in the Switch



A UNI or ENI can be an access port, a trunk port, a private VLAN port, or an 802.1Q tunnel port. It can also be a member of an EtherChannel.

When a UNI or ENI configured as an 802.1Q trunk port belongs to a UNI-ENI isolated VLAN, the VLAN on the trunk is isolated from the same VLAN ID on a different trunk port or an access port. Other VLANs on the trunk port can be of different types (private VLAN, UNI-ENI community VLAN, and so on). For example, a UNI access port and one VLAN on a UNI trunk port can belong to the same UNI-ENI isolated VLAN. In this case, isolation occurs between the UNI access port and the VLAN on the UNI trunk port. Other access ports and other VLANs on the trunk port are isolated because they belong to different VLANs.

UNIs, ENIs, and NNIs are always isolated from ports on different VLANs.

Prerequisites

- Be familiar with the information in the "Information About VLANs" section on page 3-1 and "Guidelines and Limitations" section on page 3-7.
- Ensure that your network strategy and planning for your network are complete.

Guidelines and Limitations

Follow these guidelines when creating and modifying VLANs in your network:

- The switch supports 1005 VLANs.
- Normal-range Ethernet VLANs are identified with a number between 1 and 1001. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs.
- The switch does not support Token Ring or FDDI media. The switch does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic.
- VLAN configurations for VLANs 1 to 1005 are always saved in the VLAN database and in the switch running configuration file.
- Configuration options for VLAN IDs 1006 through 4094 (extended-range VLANs) are limited to MTU, RSPAN VLAN, private VLAN, and UNI-ENI VLAN. Extended-range VLANs are not saved in the VLAN database.
- Spanning Tree Protocol (STP) is enabled by default for only NNIs on all VLANs. You can configure STP on ENIs. NNIs and ENIs in the same VLAN are in the same spanning-tree instance. The switch supports 128 spanning-tree instances. If a switch has more active VLANs than supported spanning-tree instances, spanning tree can be enabled on 128 VLANs and is disabled on the remaining VLANs. If you have already used all available spanning-tree instances on a switch, adding another VLAN creates a VLAN on that switch that is not running spanning tree. If you have the default allowed list on the trunk ports of that switch (which is to allow all VLANs), the new VLAN is carried on all trunk ports. Depending on the topology of the network, this could create a loop in the new VLAN that would not be broken, particularly if there are several adjacent switches that all have run out of spanning-tree instances. You can prevent this possibility by setting allowed lists on the trunk ports of switches that have used up their allocation of spanning-tree instances.

  If the number of VLANs on the switch exceeds the number of supported spanning-tree instances, we recommend that you configure the 802.1s Multiple STP (MSTP) on your switch to map multiple VLANs to a single spanning-tree instance. For more information about MSTP, see Chapter 12, "Configuring MSTP."

  Note MSTP is supported only on NNIs on ENIs on which STP has been enabled.

- Each routed port on the switch creates an internal VLAN for its use. These internal VLANs use extended-range VLAN numbers, and the internal VLAN ID cannot be used for an extended-range VLAN. If you try to create an extended-range VLAN with a VLAN ID that is already allocated as an internal VLAN, an error message is generated, and the command is rejected.
  - Because internal VLAN IDs are in the lower part of the extended range, we recommend that you create extended-range VLANs beginning from the highest number (4094) and moving to the lowest (1006) to reduce the possibility of using an internal VLAN ID.

  - Before configuring extended-range VLANs, enter the **show vlan internal usage** privileged EXEC command to see which VLANs have been allocated as internal VLANs.
  - If necessary, you can shut down the routed port assigned to the internal VLAN, which frees up the internal VLAN, and then create the extended-range VLAN and re-enable the port, which then uses another VLAN as its internal VLAN. See the "Creating an Extended-Range VLAN with an Internal VLAN ID" section on page 3-12.
- Although the switch supports a total of 1005 (normal-range and extended-range) VLANs, the number of routed ports, SVIs, and other configured features affects the use of the switch hardware. If you try to create an extended-range VLAN and there are not enough hardware resources available, an error message is generated, and the extended-range VLAN is rejected.

UNI-ENI VLAN

These are the guidelines for UNI-ENI VLAN configuration:

- UNI-ENI isolated VLANs have no effect on NNI ports.
- A UNI-ENI community VLAN is like a traditional VLAN except that it can include no more than a combination of eight UNIs and ENIs.
- To change a VLAN type, first enter the **vlan** *vlan-id* global configuration command to enter VLAN configuration mode:
  - To change a VLAN from UNI-ENI isolated VLAN to a private VLAN, enter the **private-vlan** VLAN configuration command.
  - To change a UNI-ENI community VLAN to a private VLAN, you must first remove the community VLAN type by entering the **no uni-vlan** VLAN configuration command. Then enter the **private-vlan** VLAN configuration command.
  - To change a VLAN from a UNI-ENI isolated VLAN to an RSPAN VLAN, enter the **rspan-vlan** VLAN configuration command.
  - To change a UNI-ENI community VLAN to an RSPAN VLAN, you must first remove the community VLAN type by entering the **no uni-vlan** VLAN configuration command. Then enter the **rspan-vlan** VLAN configuration command.
  - To change a private VLAN to a UNI-ENI VLAN, you must first remove the private VLAN type by entering the **no private-vlan** VLAN configuration command. Then enter the **uni-vlan** VLAN configuration command.
  - To change an RSPAN VLAN to a UNI-ENI VLAN, you must first remove the RSPAN VLAN type by entering the **no rspan-vlan** VLAN configuration command. Then enter the **uni-vlan** VLAN configuration command
- The switch supports a total of eight UNIs and ENIs in a community VLAN. You cannot configure a VLAN as a UNI-ENI community VLAN if more than eight UNIs and ENIs belong to the VLAN.
- If you attempt to add a UNI or ENI static-access port to a UNI-ENI community VLAN that has a combination of eight UNIs and ENIs, the configuration is refused. If a UNI or ENI dynamic access port is added to a UNI-ENI community VLAN that has eight UNIs or ENIs, the port is error-disabled.
- Use caution when configuring ENIs and UNIs in the same community VLAN. Local switching takes place between the ENIs and UNIs in the community VLAN and ENIs can support spanning tree while UNIs do not.

Default Settings

The switch supports only Ethernet interfaces. The following table shows the default configuration for Ethernet VLANs.

Note On extended-range VLANs, you can change only the MTU size, the private VLAN, the remote SPAN, and the UNI-ENI VLAN configuration. All other characteristics must remain at the default conditions.

Parameter	Default	Range
VLAN ID	1	1 to 4094 **Note** Extended-range VLANs (VLAN IDs 1006 to 4094) are not saved in the VLAN database.
VLAN name	*VLANxxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number	No range
802.10 SAID	100001 (100000 plus the VLAN ID)	1 to 4294967294
MTU size	1500	1500 to 9198
Translational bridge 1	0	0 to 1005
Translational bridge 2	0	0 to 1005
VLAN state	active	active, suspend
Remote SPAN	disabled	enabled, disabled
Private VLANs	none configured	2 to 1001, 1006 to 4094
UNI-ENI VLAN	UNI-ENI isolated VLAN	2 to 1001, 1006 to 4094 VLAN 1 is always a UNI-ENI isolated VLAN.

Configuring VLANs

You use VLAN configuration mode, accessed by entering the **vlan** global configuration command, to create VLANs and to modify some parameters. You use the interface configuration mode to define the port membership mode and to add and remove ports from VLANs. The results of these commands are written to the running-configuration file, and you can display the file by entering the **show running-config** privileged EXEC command.

This section includes the following topics:

- Creating or Modifying an Ethernet VLAN, page 3-10
- Assigning Static-Access Ports to a VLAN, page 3-11
- Creating an Extended-Range VLAN with an Internal VLAN ID, page 3-12
- Configuring UNI-ENI VLANs, page 3-14

For more efficient management of the MAC address table space available on the switch, you can control which VLANs learn MAC addresses by disabling MAC address learning on specific VLANs. See the “Disabling MAC Address Learning on a VLAN” section of the “Administering the Switch” chapter in the *System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches* for more information.

Creating or Modifying an Ethernet VLAN

To access VLAN configuration mode, enter the **vlan** global configuration command with a VLAN ID. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. You can use the default VLAN configuration (see the “Default Settings” section on page 3-9) or enter commands to configure the VLAN.

Note Extended-range VLANs use the default Ethernet VLAN characteristics and the MTU, the private VLAN, the RSPAN, and the UNI-ENI VLAN configurations are the only parameters you can change.

For more information about commands available in this mode, see the **vlan** command description in the command reference for this release. When you have finished the configuration, you must exit VLAN configuration mode for the configuration to take effect. To display the VLAN configuration, enter the **show vlan** privileged EXEC command.

The configurations of VLAN IDs 1 to 1005 are always saved in the VLAN database (vlan.dat file) with a VLAN number and name and in the switch running configuration file. Extended-range VLANs are not saved in the VLAN database; they are saved in the switch running configuration file. You can save the VLAN configuration in the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

BEFORE YOU BEGIN

Before you create an extended-range VLAN, verify that the VLAN ID is not used internally by entering the **show vlan internal usage** privileged EXEC command. If the VLAN ID is used internally and you want to release it, go to the “Creating an Extended-Range VLAN with an Internal VLAN ID” section on page 3-12 before creating the extended-range VLAN.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vlan** *vlan-id*	Enter a VLAN ID, and enter VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. The available VLAN ID range for this command is 1 to 4094. **Note** When you create a new VLAN, by default the VLAN is a UNI-ENI isolated VLAN.

	Command	Purpose
Step 3	**name** *vlan-name*	(Optional and supported on normal-range VLANs only) Enter a name for the VLAN. If no name is entered for the VLAN, the default in the VLAN database is to append the *vlan-id* with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4.
Step 4	**mtu** *mtu-size*	(Optional) Change the MTU size.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show vlan** {**name** *vlan-name* | **id** *vlan-id*}	Verify your entries. The **name** option is only valid for VLAN IDs 1 to 1005.
Step 7	**copy running-config startup config**	(Optional) Save the configuration in the switch startup configuration file.

To delete a VLAN, use the **no vlan** *vlan-id* global configuration command. You cannot delete VLAN 1 or VLANs 1002 to 1005.

Caution When you delete a VLAN, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN.

To return the VLAN name to the default settings, use the **no name** or **no mtu** VLAN configuration command.

EXAMPLE

This example shows how to create Ethernet VLAN 20, name it *test20*, and add it to the VLAN database:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

This example shows how to create a new extended-range VLAN with all default characteristics, enter config-vlan mode, and save the new VLAN in the switch startup configuration file:

```
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

Assigning Static-Access Ports to a VLAN

You can assign a static-access port to a VLAN.

Note If you assign an interface to a VLAN that does not exist, the new VLAN is created. (See the "Creating or Modifying an Ethernet VLAN" section on page 3-10.)

BEFORE YOU BEGIN

Review the "Information About VLANs" section on page 3-1 and "Guidelines and Limitations" section on page 3-7.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter the interface to add to the VLAN.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	**switchport mode access**	Define the VLAN membership mode for the port (Layer 2 access port).
Step 5	**switchport access vlan** *vlan-id*	Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config interface** *interface-id*	Verify the VLAN membership mode of the interface.
Step 8	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Administrative Mode* and the *Access Mode VLAN* fields of the display.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command.

EXAMPLE

This example shows how to configure a port as an access port in VLAN 2:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
```

Creating an Extended-Range VLAN with an Internal VLAN ID

If you enter an extended-range VLAN ID that is already assigned to an internal VLAN, an error message appears, and the extended-range VLAN is rejected. To manually release an internal VLAN ID, you must temporarily shut down the routed port that is using the internal VLAN ID.

BEFORE YOU BEGIN

Review the “Guidelines and Limitations” section on page 3-7.

DETAILED STEPS

	Command	Purpose
Step 1	**show vlan internal usage**	Display the VLAN IDs being used internally by the switch. If the VLAN ID that you want to use is an internal VLAN, the display shows the routed port that is using the VLAN ID. Enter that port number in Step 3.
Step 2	**configure terminal**	Enter global configuration mode.
Step 3	**interface** *interface-id*	Specify the interface ID for the routed port that is using the VLAN ID, and enter interface configuration mode.
Step 4	**shutdown**	Shut down the port to release the internal VLAN ID.
Step 5	**exit**	Return to global configuration mode.
Step 6	**vlan** *vlan-id*	Enter the new extended-range VLAN ID, and enter config-vlan mode.
Step 7	**exit**	Exit from config-vlan mode, and return to global configuration mode.
Step 8	**interface** *interface-id*	Specify the interface ID for the routed port that you shut down in Step 4, and enter interface configuration mode.
Step 9	**no shutdown**	Re-enable the routed port. It will be assigned a new internal VLAN ID.
Step 10	**end**	Return to privileged EXEC mode.
Step 11	**copy running-config startup config**	(Optional) Save your entries in the switch startup configuration file.

EXAMPLE

This example shows how to release internal VLAN ID 1030:

```
Switch# show vlan internal usage

VLAN Usage
---- --------------------
1025 -
1026 -
1027 -
1028 -
1029 Port-channel6
1030 GigabitEthernet1/2
1032 FastEthernet3/20
1033 FastEthernet3/21
1129 -
Switch# configure terminal
Switch(config)# interface GigabitEthernet1/2
Switch(config-if)# shutdown
Switch(config-if)# exit
Switch(config)# vlan 1030
Switch(config-vlan)# exit
Switch(config)# interface GigabitEthernet1/2
Switch(config-if)# no shutdown
Switch(config-if)# end
```

Configuring UNI-ENI VLANs

By default, every VLAN configured on the switch is a UNI-ENI isolated VLAN. You can change VLAN configuration to that of a UNI-ENI community VLAN, a private VLAN, or an RSPAN VLAN. You can also change the configuration of one of these VLANs to the default of a UNI-ENI isolated VLAN.

For procedures for configuring private VLANs or RSPAN VLANs, see Chapter 7, "Configuring Private VLANs" and the "Configuring SPAN and RSPAN" chapter in the *System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.

BEFORE YOU BEGIN

Review the "UNI-ENI VLANs" section on page 3-5 and the UNI-ENI VLAN configuration guidelines in the "Guidelines and Limitations" section on page 3-7.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vlan** *vlan-id*	Enter a VLAN ID, and enter VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. By default, the VLAN is a UNI-ENI isolated VLAN. **Note** The available VLAN ID range for this command is 1 to 4094.
Step 3	**uni-vlan** {**community** | **isolated**}	Configure the UNI-ENI VLAN type. • Enter **community** to change from the default to a UNI-ENI community VLAN. • Enter **isolated** to return to the default UNI-ENI isolated VLAN. **Note** VLAN 1 is always a UNI-ENI isolated VLAN; you cannot configure VLAN 1 as a UNI-ENI community VLAN. The reserved VLANs 1002 to 1005 are not Ethernet VLANs.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show vlan uni-vlan** [**type**]	Display UNI-ENI VLAN information. Enter **type** (optional) to see only the VLAN ID and type of UNI-ENI VLAN.
Step 6	**copy running-config startup config**	(Optional) Save the configuration in the switch startup configuration file.

Use the **no uni-vlan** VLAN configuration command to return to the default (UNI-ENI isolated VLAN). Entering **uni-vlan isolated** command has the same effect as entering the no **uni-vlan** VLAN configuration command. The **show vlan** and **show vlan** *vlan-id* privileged EXEC commands also display UNI-ENI VLAN information, but only UNI-ENI community VLANs appear. To display both isolated and community VLANs, use the **show vlan uni-vlan type** command.

EXAMPLE

This example configures VLAN 20 as a community VLAN:

```
Switch(config)# vlan 20
Switch (config-vlan)# uni-vlan community
Switch (config-vlan)# end
```

Verifying Configuration

Command	Purpose
show interfaces [**vlan** *vlan-id*]	Display characteristics for all interfaces or for the specified VLAN configured on the switch.
show vlan [**id** *vlan-id*]	Display parameters for all VLANs or the specified VLAN on the switch.
show vlan [*vlan-name*] **uni-vlan type**	Display UNI-ENI isolated or UNI-ENI community VLANs by VLAN name.
show vlan uni-vlan	Display UNI-ENI community VLANs and associated ports on the switch.
show vlan uni-vlan type	Display UNI-ENI isolated and UNI-ENI community VLANs on the switch by VLAN ID.

Configuration Example

This example shows how to create Ethernet VLAN 20, name it *test20*, and add it to the VLAN database:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

This example shows how to create a new extended-range VLAN with all default characteristics, enter config-vlan mode, and save the new VLAN in the switch startup configuration file:

```
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

This example shows how to configure a port as an access port in VLAN 2:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
```

This example shows how to release internal VLAN ID 1030:

```
Switch# show vlan internal usage

VLAN Usage
---- --------------------
1025 -
1026 -
1027 -
1028 -
```

```
1029 Port-channel6
1030 GigabitEthernet1/2
1032 FastEthernet3/20
1033 FastEthernet3/21
1129 -
Switch# configure terminal
Switch(config)# interface GigabitEthernet1/2
Switch(config-if)# shutdown
Switch(config-if)# exit
Switch(config)# vlan 1030
Switch(config-vlan)# exit
Switch(config)# interface GigabitEthernet1/2
Switch(config-if)# no shutdown
Switch(config-if)# end
```

This example configures VLAN 20 as a community VLAN:

```
Switch(config)# vlan 20
Switch (config-vlan)# uni-vlan community
Switch (config-vlan)# end
```

Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS LAN Switching Command Reference
- Cisco IOS Interface and Hardware Component Command Reference
- Interfaces Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches
- System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520 Switch	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

Configuring VLAN Trunks

This chapter provides the following information about configuring VLAN trunks on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*:

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 4-13.

Information About Trunks

A trunk is a point-to-point link between one or more Ethernet switch interfaces and another networking device such as a router or a switch. Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network. The switch supports the 802.1Q industry-standard trunking encapsulation.

You can configure a trunk on a single Ethernet interface or on an EtherChannel bundle. For more information about EtherChannels, see the "Configuring EtherChannels and Link State Tracking" chapter in the *High Availability and Redundancy Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.

Ethernet interfaces support different trunking modes (see Table 4-1). You can set an interface as trunking or nontrunking.

- If you do not intend to trunk across links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking, use the **switchport mode trunk** interface configuration command to change the interface to a trunk.

Table 4-1 Layer 2 Interface Modes

Mode	Function
switchport mode access	Puts the interface (access port) into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface regardless of whether or not the neighboring interface is a trunk interface. This is the default mode.
switchport mode trunk	Puts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link. The interface becomes a trunk interface even if the neighboring interface is not a trunk interface.
switchport mode dot1q-tunnel	Configures the interface as a tunnel (nontrunking) port to be connected in an asymmetric link with an 802.1Q trunk port. The 802.1Q tunneling is used to maintain customer VLAN integrity across a service provider network. See Chapter 10, "Configuring Layer 2 Protocol Tunneling," for more information on tunnel ports.
switchport mode private-vlan	Configure the interface as a private VLAN host or promiscuous port (only NNIs can be configured as promiscuous ports). For information about private VLANs, see Chapter 7, "Configuring Private VLANs."

Prerequisites

- Be familiar with the information in the "Information About Trunks" section on page 4-1 and "Guidelines and Limitations" section on page 4-2.
- Ensure that your network strategy and planning for your network are complete.

Guidelines and Limitations

The 802.1Q trunks impose these limitations on the trunking strategy for a network:

- In a network of Cisco switches connected through 802.1Q trunks, the switches maintain one spanning-tree instance for each VLAN allowed on the trunks. Non-Cisco devices might support one spanning-tree instance for all VLANs.

  When you connect a Cisco switch to a non-Cisco device through an 802.1Q trunk, the Cisco switch combines the spanning-tree instance of the VLAN of the trunk with the spanning-tree instance of the non-Cisco 802.1Q switch. However, spanning-tree information for each VLAN is maintained by Cisco switches separated by a cloud of non-Cisco 802.1Q switches. The non-Cisco 802.1Q cloud separating the Cisco switches is treated as a single trunk link between the switches.
- Make sure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.
- Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can potentially cause spanning-tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk or disable spanning tree on every VLAN in the network. Make sure that your network is loop-free before disabling spanning tree.

Interaction with Other Features

Trunking interacts with other features in these ways:

- A trunk port cannot be a secure port.
- A trunk port cannot be a tunnel port.
- Trunk ports can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration. When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, the switch propagates the setting that you entered to all ports in the group:
  - allowed-VLAN list.
  - STP port priority for each VLAN.
  - STP Port Fast setting.

Note STP is supported by default on NNIs, but must be enabled on ENIs. STP is not supported on UNIs.

  - trunk status: if one port in a port group ceases to be a trunk, all ports cease to be trunks.
- If you try to enable 802.1x on a trunk port, an error message appears, and 802.1x is not enabled. If you try to change the mode of an 802.1x-enabled port to trunk, the port mode is not changed.

Default Settings

The following table shows the default Layer 2 Ethernet interface VLAN configuration.

Feature	Default Setting
Interface mode	**switchport mode access**
Allowed VLAN range	VLANs 1 to 4094
Default VLAN (for access ports)	VLAN 1
Native VLAN (for 802.1Q trunks)	VLAN 1

Configuring VLAN Trunks

This section includes the following topics:

Configuring a Trunk Port

Follow this procedure to configure a a port as an 802.1Q trunk port.

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 4-2.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured for trunking, and enter interface configuration mode.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	**switchport mode trunk**	Configure the interface as a Layer 2 trunk.
Step 5	**switchport access vlan** *vlan-id*	(Optional) Specify the default VLAN, which is used if the interface stops trunking.
Step 6	**switchport trunk native vlan** *vlan-id*	Specify the native VLAN for 802.1Q trunks.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show interfaces** *interface-id* **switchport**	Display the switchport configuration of the interface in the *Administrative Mode* field of the display.
Step 9	**show interfaces** *interface-id* **trunk**	Display the trunk configuration of the interface.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command. To reset all trunking characteristics of a trunking interface to the defaults, use the **no switchport trunk** interface configuration command. To disable trunking, use the **switchport mode access** interface configuration command to configure the port as a static-access port.

EXAMPLE

This example shows how to configure a port as an 802.1Q trunk with VLAN 33 as the native VLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 33
Switch(config-if)# end
```

Defining the Allowed VLANs on a Trunk

By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs, 1 to 4094, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk. To restrict the traffic a trunk carries, use the **switchport trunk allowed vlan remove** *vlan-list* interface configuration command to remove specific VLANs from the allowed list.

Note VLAN 1 is the default VLAN on all trunk ports in all Cisco switches, and it has previously been a requirement that VLAN 1 always be enabled on every trunk link. The VLAN 1 minimization feature allows you to disable VLAN 1 on any individual VLAN trunk link so that no user traffic (including spanning-tree advertisements) is sent or received on VLAN 1. You do this by removing VLAN 1 from the allowed VLAN list.

To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), Port Aggregation Protocol (PAgP), and Link Aggregation Control Protocol (LACP) in VLAN 1.

If a trunk port with VLAN 1 disabled is converted to a nontrunk port, it is added to the access VLAN. If the access VLAN is set to 1, the port is added to VLAN 1, regardless of the **switchport trunk allowed** setting. The same is true for any VLAN that has been disabled on the port.

A trunk port can become a member of a VLAN if the VLAN is enabled and if the VLAN is in the allowed list for the port.

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 4-2.

DETAILED STEPS

Beginning in privileged EXEC mode, follow these steps to modify the allowed list of an IEEE 802.1Q trunk:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	**switchport mode trunk**	Configure the interface as a VLAN trunk port.

	Command	Purpose
Step 5	**switchport trunk allowed vlan** {**add** | **all** | **except** | **remove**} *vlan-list*	(Optional) Configure the list of VLANs allowed on the trunk. For explanations about using the **add**, **all**, **except**, and **remove** keywords, see the command reference for this release. The *vlan-list* parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated VLAN parameters or in hyphen-specified ranges. All VLANs are allowed by default.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Trunking VLANs Enabled* field of the display.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default allowed VLAN list of all VLANs, use the **no switchport trunk allowed vlan** interface configuration command.

EXAMPLE

This example shows how to remove VLAN 2 from the allowed VLAN list on a port:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
```

Configuring the Native VLAN for Untagged Traffic

A trunk port configured with 802.1Q tagging can receive both tagged and untagged traffic. By default, the switch forwards untagged traffic in the native VLAN configured for the port. The native VLAN is VLAN 1 by default. If a packet has a VLAN ID that is the same as the sending port native VLAN ID, the packet is sent untagged; otherwise, the switch sends the packet with a tag.

Note The native VLAN can be assigned any VLAN ID.

For information about 802.1Q configuration issues, see the "Guidelines and Limitations" section on page 4-2.

BEFORE YOU BEGIN

Configure a trunk port as described in the "Configuring a Trunk Port" procedure on page 4-4.

DETAILED STEPS

Beginning in privileged EXEC mode, follow these steps to configure the native VLAN on an IEEE 802.1Q trunk:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Define the interface that is configured as the 802.1Q trunk, and enter interface configuration mode.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled and NNIs are enabled.
Step 4	**switchport trunk native vlan** *vlan-id*	Configure the VLAN that is sending and receiving untagged traffic on the trunk port. For *vlan-id*, the range is 1 to 4094.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Trunking Native Mode VLAN* field.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default native VLAN, VLAN 1, use the **no switchport trunk native vlan** interface configuration command.

EXAMPLE

This example configures VLAN 100 as the native VLAN for the trunk port:

```
Switch(config)# interface fastethernet5/1
Switch(config-if)# switchport trunk native vlan 100
Switch(config-if)# end
```

Configuring Trunk Ports for Load Sharing

Load sharing divides the bandwidth supplied by parallel trunks that connect switches. To avoid loops, STP normally blocks all but one parallel link between switches. Using load sharing, you divide the traffic between the links according to the VLAN to which the traffic belongs.

You configure load sharing on trunk ports that have STP enabled by using STP port priorities or STP path costs. For load sharing using STP port priorities, both load-sharing links must be connected to the same switch. For load sharing using STP path costs, each load-sharing link can be connected to the same switch or to two different switches. For more information about STP, see Chapter 11, "Configuring STP."

Load Sharing Using STP Port Priorities

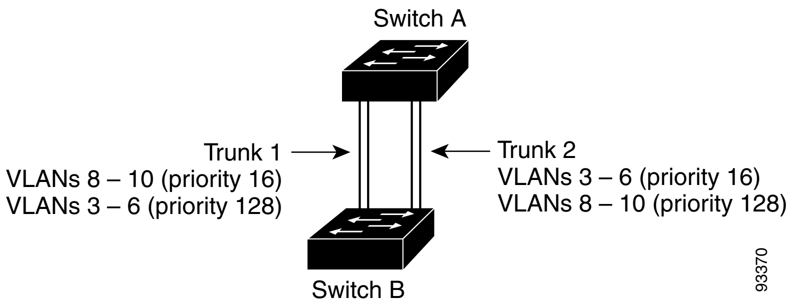
When two ports on the same switch form a loop, the switch uses the STP port priority to decide which port is enabled and which port is in a blocking state. You can set the priorities on a parallel STP trunk port so that the port carries all the traffic for a given VLAN. The trunk port with the higher priority (lower values) for a VLAN is forwarding traffic for that VLAN. The trunk port with the lower priority (higher values) for the same VLAN remains in a blocking state for that VLAN. One trunk port sends or receives all traffic for the VLAN.

Figure 4-1 shows two trunks connecting supported switches. In this example, the switches are configured as follows:

- VLANs 8 through 10 are assigned a port priority of 16 on Trunk 1.
- VLANs 3 through 6 retain the default port priority of 128 on Trunk 1.
- VLANs 3 through 6 are assigned a port priority of 16 on Trunk 2.
- VLANs 8 through 10 retain the default port priority of 128 on Trunk 2.

In this way, Trunk 1 carries traffic for VLANs 8 through 10, and Trunk 2 carries traffic for VLANs 3 through 6. If the active trunk fails, the trunk with the lower priority takes over and carries the traffic for all of the VLANs. No duplication of traffic occurs over any trunk port.

Figure 4-1 Load Sharing by Using STP Port Priorities


Switch A
Trunk 1
VLANs 8 – 10 (priority 16)
VLANs 3 – 6 (priority 128)
Trunk 2
VLANs 3 – 6 (priority 16)
VLANs 8 – 10 (priority 128)
Switch B
93370

Follow this procedure on Switch A to configure the network shown in Figure 4-1. Note that you can use any interface numbers; those shown are examples only.

BEFORE YOU BEGIN

If you configure the port as an ENI, you must also enable STP on the port by entering the **spanning-tree** interface configuration command.

DETAILED STEPS

	Command	Purpose
Step 1	**show vlan**	Verify that the referenced VLANs exist on Switch A. If not, create the VLANs by entering the VLAN IDs.
Step 2	**configure terminal**	Enter global configuration mode.
Step 3	**interface gigabitethernet 0/1**	Define the interface to be configured as the Trunk 1 interface, and enter interface configuration mode.
Step 4	**port-type** {**nni** | **eni**}	Configure the interface as an NNI or ENI. UNIs do not support STP.
Step 5	**switchport mode trunk**	Configure the port as a trunk port.
Step 6	**spanning-tree vlan 8-10 port-priority 16**	Assign the port priority of 16 for VLANs 8 through 10 on Trunk 1.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show interfaces gigabitethernet 0/1 switchport**	Verify the port configuration.
Step 9	**configure terminal**	Enter global configuration mode.

	Command	Purpose
Step 10	**interface gigabitethernet 0/2**	Define the interface to be configured as the Trunk 2 interface, and enter interface configuration mode.
Step 11	**port-type** {**nni** | **eni**}	Configure the interface as an NNI or ENI. UNIs do not support STP. If you configure the port as an ENI, you must also enable STP on the port by entering the **spanning-tree** interface configuration command.
Step 12	**switchport mode trunk**	Configure the port as a trunk port.
Step 13	**spanning-tree vlan 3-6 port-priority 16**	Assign the port priority of 16 for VLANs 3 through 6 on Trunk 2.
Step 14	**end**	Return to privileged EXEC mode.
Step 15	**show interfaces gigabitethernet 0/2 switchport**	Verify the port configuration.
Step 16	**show running-config**	Verify your entries.
Step 17	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Follow the same steps on Switch B to configure the trunk port for Trunk 1 with a spanning-tree port priority of 16 for VLANs 8 through 10, and configure the trunk port for Trunk 2 with a spanning-tree port priority of 16 for VLANs 3 through 6.

EXAMPLE

This example configures Switch A for the network shown in Figure 4-1.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# port-type nni
Switch(config-if)# switchport mode trunk
Switch(config-if)# spanning-tree vlan 8-10 port-priority 16
Switch(config-if)# end
Switch# show interfaces gigabitethernet 0/1 switchport
.
.
.
Switch# configure terminal
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# port-type nni
Switch(config-if)# switchport mode trunk
Switch(config-if)# spanning-tree vlan 3-6 port-priority 16
Switch(config-if)# end
Switch# show interfaces gigabitethernet 0/2 switchport
.
.
.
```

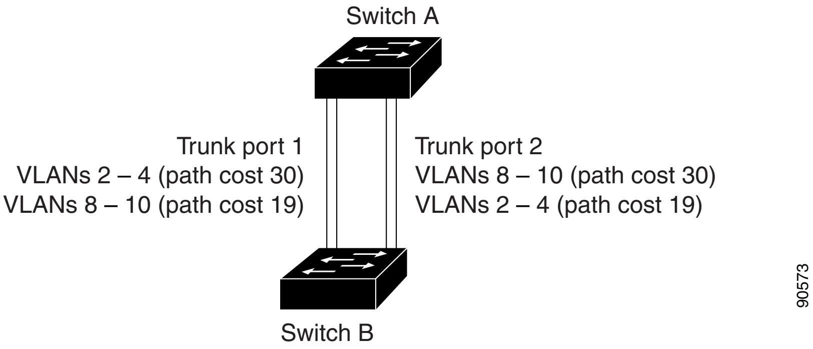
Load Sharing Using STP Path Cost

You can configure parallel trunks to share VLAN traffic by setting different path costs on a trunk and associating the path costs with different sets of VLANs, blocking different ports for different VLANs. You can assign lower cost values to interfaces that you want selected first and higher cost values that you want selected last. (See the "Configuring Path Cost" section on page 11-22.) The VLANs keep the traffic separate and maintain redundancy in the event of a lost link.

In Figure 4-2, Trunk ports 1 and 2 are configured as 100Base-T ports. These VLAN path costs are assigned:

- VLANs 2 through 4 are assigned a path cost of 30 on Trunk port 1.
- VLANs 8 through 10 retain the default 100Base-T path cost on Trunk port 1 of 19.
- VLANs 8 through 10 are assigned a path cost of 30 on Trunk port 2.
- VLANs 2 through 4 retain the default 100Base-T path cost on Trunk port 2 of 19.

Figure 4-2 Load-Sharing Trunks with Traffic Distributed by Path Cost


Switch A
Trunk port 1
VLANs 2 – 4 (path cost 30)
VLANs 8 – 10 (path cost 19)
Trunk port 2
VLANs 8 – 10 (path cost 30)
VLANs 2 – 4 (path cost 19)
90573
Switch B

Follow this procedure to configure the network shown in Figure 4-2.

BEFORE YOU BEGIN

If you configure the port as an ENI, you must also enable STP on the port by entering the **spanning-tree** interface configuration command.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode on Switch A.
Step 2	**interface fastethernet0/1**	Define the interface to be configured as Trunk port 1, and enter interface configuration mode.
Step 3	**port-type** {**nni** | **eni**}	Configure the interface as an NNI or ENI. UNIs do not support STP.
Step 4	**switchport mode trunk**	Configure the port as a trunk port.
Step 5	**exit**	Return to global configuration mode.
Step 6	**interface fastethernet0/2**	Define the interface to be configured as Trunk port 2, and enter interface configuration mode.
Step 7	**port-type** {**nni** | **eni**}	Configure the interface as an NNI or ENI. UNIs do not support STP.
Step 8	**switchport mode trunk**	Configure the port as a trunk port.
Step 9	**end**	Return to privileged EXEC mode.
Step 10	**show running-config**	Verify your entries. In the display, make sure that the interfaces configured in Steps 2 and 7 are configured as trunk ports.

	Command	Purpose
Step 11	**show vlan**	Verify that VLANs 2 through 4 and 8 through 10 are configured on Switch A. If not, create these VLANs.
Step 12	**configure terminal**	Enter global configuration mode.
Step 13	**interface fastethernet0/1**	Enter interface configuration mode for Trunk port 1.
Step 14	**spanning-tree vlan 2-4 cost 30**	Set the spanning-tree path cost to 30 for VLANs 2 through 4.
Step 15	**exit**	Return to global configuration mode.
Step 16	**interface fastethernet0/2**	Enter interface configuration mode for Trunk port 2.
Step 17	**spanning-tree vlan 8-10 cost 30**	Set the spanning-tree path cost to 30 for VLANs 8 through 10.
Step 18	**end**	Return to privileged EXEC mode.
Step 19	**show running-config**	Verify your entries. In the display, verify that the path costs are set correctly for both trunk interfaces.
Step 20	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Follow the same steps on Switch B to configure the trunk port for Trunk 1 with a path cost of 30 for VLANs 2 through 4, and configure the trunk port for Trunk 2 with a path cost of 30 for VLANs 8 through 10.

EXAMPLE

This examples configures Switch A for the network shown in Figure 4-2.

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# port-type nni
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
Switch(config)# interface fastethernet0/2
Switch(config-if)# port-type nni
Switch(config-if)# switchport mode trunk
Switch(config-if)# end
Switch# show running-config
.
.
.
Switch# show vlan
.
.
.
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# spanning-tree vlan 2-4 cost 30
Switch(config-if)# exit
Switch(config)# interface fastethernet0/2
Switch(config-if)# spanning-tree vlan 8-10 cost 30
Switch(config-if)# end
Switch# show running config

.
.
.
```

Verifying Configuration

Command	Purpose
show interfaces *interface-id* **switchport**	Display the switchport configuration of the interface.
show interfaces *interface-id* **trunk**	Display the trunk configuration of the interface.
show running-config	Display interfaces configured as trunk ports.

Configuration Example

This example shows how to configure a port as an 802.1Q trunk with VLAN 33 as the native VLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 33
Switch(config-if)# end
```

This example shows how to remove VLAN 2 from the allowed VLAN list on a port:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
```

This example configures VLAN 100 as the native VLAN for the trunk port:

```
Switch(config)# interface fastethernet5/1
Switch(config-if)# switchport trunk native vlan 100
Switch(config-if)# end
```

This example configures Switch A for the network shown in Figure 4-1.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# port-type nni
Switch(config-if)# switchport mode trunk
Switch(config-if)# spanning-tree vlan 8-10 port-priority 16
Switch(config-if)# end
Switch# show interfaces gigabitethernet 0/1 switchport
.
.
.
Switch# configure terminal
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# port-type nni
Switch(config-if)# switchport mode trunk
Switch(config-if)# spanning-tree vlan 3-6 port-priority 16
Switch(config-if)# end
Switch# show interfaces gigabitethernet 0/2 switchport
.
.
.
```

This examples configures Switch A for the network shown in Figure 4-2.

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# port-type nni
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
Switch(config)# interface fastethernet0/2
Switch(config-if)# port-type nni
Switch(config-if)# switchport mode trunk
Switch(config-if)# end
Switch# show running-config
.
.
.
Switch# show vlan
.
.
.
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# spanning-tree vlan 2-4 cost 30
Switch(config-if)# exit
Switch(config)# interface fastethernet0/2
Switch(config-if)# spanning-tree vlan 8-10 cost 30
Switch(config-if)# end
Switch# show running config

.
.
.
```

Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS LAN Switching Command Reference
- Cisco IOS Interface and Hardware Component Command Reference
- High Availability and Redundancy Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520 Switch	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

CHAPTER 5

Configuring Asymmetric VLAN Mapping

This chapter describes how to configure the asymmetric VLAN mapping feature for the Cisco 2520 Connected Grid Switch (CGS 2520). This chapter includes the following sections:

Note VLAN Mapping is not supported on the Cisco Industrial Ethernet 2000U Series (IE 2000U) switch or the Ethernet Switch Module (ESM) for CGR 2010.

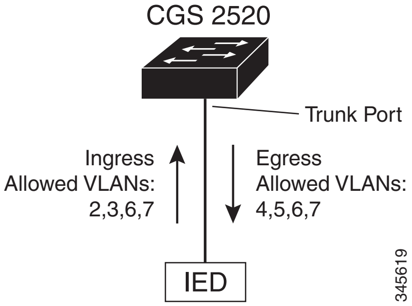
Information About Asymmetric VLAN Mapping

The Asymmetric VLAN mapping feature provides a method for restricting traffic on VLAN trunk ports. The feature lets you specify lists of VLANs that are allowed to forward traffic on the trunk port in the ingress direction, egress direction, or in both directions.

This feature is useful in a utility substation environment where a VLAN trunk is connected between a Cisco CGS 2520 switch and an intelligent electronic device (IED). The trunk port on the Cisco CGS 2520 can be configured to allow ingress traffic for a given VLAN, such as generic object oriented substation events (GOOSE) messages from the IED, and the trunk port can be configured to allow traffic for specific VLAN IDs in the egress direction, allowing the IED to subscribe to GOOSE messages with those VLAN IDs. All other VLAN traffic on the trunk port can be blocked.

In the example shown in Figure 5-1, there are six VLANs (2, 3, 4, 5, 6, 7) configured on a Cisco CGS 2520 switch. Using the asymmetric VLAN mapping feature on a trunk port, packets tagged with VLANs 2 and 3 can only enter the system through that interface, packets tagged with VLANs 4 and 5 can only go out of the system (but cannot enter the system), and packets tagged with VLANs 6 and 7 can both enter and exit the system. Any other tagged packets are dropped at the interface level where this feature is configured.

Figure 5-1 Asymmetric VLAN Mapping Between a Cisco CGS 2520 and an IED



Guidelines and Limitations

These are the guidelines for configuring asymmetric VLAN mapping:

- The asymmetric VLAN mapping feature is applicable only to Layer 2 trunk ports that are in NNI mode.
- The asymmetric VLAN mapping feature should only be configured on interfaces facing IEDs.
- The feature operates at the VLAN level, so it is applicable to all of the tagged frames received on the interface where the feature is configured. For non-tagged frames, native VLAN functionality is applied.
- VLANs must already exist on the switch prior to being included in the allowed ingress, egress, or bidirectional VLAN lists.
- The maximum number of VLANs that can be included in the allowed ingress, egress, or bidirectional VLAN lists for all interfaces on the switch is 945.
- If the ternary content addressable memory (TCAM) table on the switch is full, then it is not possible to configure asymmetric VLAN mapping.

Interaction with Other Features

The asymmetric VLAN mapping feature is configured on interfaces facing IEDs, so all other Layer 2 control protocols, such as Spanning Tree BPDUs, CDP, and VTP packets should not be exchanged between the interface and an attached IED.

When the asymmetric VLAN mapping feature is enabled on an interface, CDP, STP, and VTP are disabled and cannot be configured on the interface until any configuration statements for asymmetric VLAN mapping are removed. In addition, the **no switchport** and **switchport mode access** configuration statements are not allowed when configuration statements for asymmetric VLAN mapping are present on the interface.

When the asymmetric VLAN mapping feature is configured for an interface, the VLAN mapping feature (VLAN ID translation) and the allowed VLAN feature cannot be configured for that interface.

Default Settings

Parameters	Default
Asymmetric VLAN mapping feature on VLAN trunk ports	Disabled

Configuring Asymmetric VLAN Mapping

Beginning in privileged EXEC mode, follow these steps to configure asymmetric VLAN mapping:

	Command	Purpose
Step 1	**show vlan**	Verify that the VLANs for which you are configuring mapping rules exist on the switch. If not, create the VLANs on the switch.
Step 2	**interface** *type slot/port*	Specify the interface to be configured as the trunk interface, and enter interface configuration mode. The *type* can be **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.
Step 3	**port-type nni**	Configure the interface as an NNI. Asymmetric VLAN mapping is supported only on NNI ports.
Step 4	**switchport mode trunk**	Configure the port as a trunk port.
Step 5	**switchport trunk allowed asymmetric-vlan bidirectional** {**add** | **except** | **none** | **remove**} *vlan-list*	Specifies which of the VLANs configured on the switch are allowed to send traffic through the trunk port in both the ingress and egress directions. The **add** keyword adds VLANs to the current list. The **except** keyword indicates all VLANs except those specified by *vlan-list*. The **none** keyword specifies none of the VLANs. The **remove** keyword removes VLANs from the current list. The *vlan-list* parameter is either a single VLAN number from 1 to 4094; a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen; or a comma-separated list of VLANs. Do not enter any spaces between comma-separated VLANs or in hyphen-specified ranges.
Step 6	**switchport trunk allowed asymmetric-vlan ingress** {**add** | **except** | **none** | **remove**} *vlan-list*	Specifies which of the VLANs configured on the switch are allowed to send traffic through the trunk port in the ingress direction; that is, from the IED to the switch. Traffic coming into the trunk port from all other VLANs is blocked. See step 5 for the description of the **add**, **except**, **none**, **remove**, and *vlan-list* parameters.

	Command	Purpose
Step 7	**switchport trunk allowed asymmetric-vlan egress** {**add** | **except** | **none** | **remove**} *vlan-list*	Specifies which of the VLANs configured on the switch are allowed to send traffic through the trunk port in the egress direction; that is, from the switch to the IED. Traffic from all other VLANs is blocked from exiting the trunk port. See step 5 for the description of the **add**, **except**, **none**, **remove**, and *vlan-list* parameters.
Step 8	**no vtp**	Disable VTP. VTP cannot be configured on the same interface where asymmetric VLAN mapping is configured.
Step 9	**no cdp enable**	Disable CDP. CDP cannot be configured on the same interface where asymmetric VLAN mapping is configured.
Step 10	**exit**	Return to global configuration mode.

The following example shows how to configure asymmetric VLAN mapping for a Fast Ethernet port connected to an IED. The switch has six VLANs configured on it. A trunk port is configured on the Fast Ethernet port. Traffic for VLANs 6 and 7 is allowed in both the ingress and egress direction on the trunk port; traffic for VLANs 2 and 3 is allowed from the IED to the switch; traffic for VLANs 4 and 5 is allowed from the switch to the IED. Traffic from any other VLANs is blocked at the port.

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# port-type nni
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed asymmetric-vlan bidirectional 6,7
Switch(config-if)# switchport trunk allowed asymmetric-vlan ingress 2,3
Switch(config-if)# switchport trunk allowed asymmetric-vlan egress 4,5
Switch(config-if)# no vtp
Switch(config-if)# no cdp enable
Switch(config-if)# exit
```

Verifying Configuration

Command	Purpose
show vlan asymmetric	Display the asymmetric VLAN mapping configuration in summary

Feature History

Platform	First Supported Release
CGS 2520 Switch	Cisco IOS Release 15.0(2)ED

CHAPTER 6

Configuring VMPS

This chapter describes how to configure the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*, as a client of the VLAN Membership Policy Server (VMPS).

The VLAN Query Protocol (VQP) supports dynamic-access ports, which are not permanently assigned to a VLAN, but give VLAN assignments based on the MAC source addresses seen on the port.

Note Only UNIs and ENIs can be configured as dynamic-access ports; NNIs cannot take part in VQP.

Each time an unknown MAC address is seen, the switch sends a VQP query to a remote VMPS. The query includes the newly seen MAC address and the port on which it was seen. The VMPS responds with a VLAN assignment for the port. The switch cannot be a VMPS server but can act as a client to the VMPS and communicate with it through VQP.

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 6-61.

This chapter includes the following sections:

Information About VMPS

Each time the client switch receives the MAC address of a new host, it sends a VQP query to the VMPS. When the VMPS receives this query, it searches its database for a MAC-address-to-VLAN mapping. The server response is based on this mapping and whether or not the server is in open or secure mode. In secure mode, the server shuts down the port when an illegal host is detected. In open mode, the server simply denies the host access to the port.

If the port is currently *unassigned* (that is, it does not yet have a VLAN assignment), the VMPS provides one of these responses:

- If the host is allowed on the port, the VMPS sends the client a *vlan-assignment* response containing the assigned VLAN name and allowing access to the host.
- If the host is not allowed on the port and the VMPS is in open mode, the VMPS sends an *access-denied* response.
- If the VLAN is not allowed on the port and the VMPS is in secure mode, the VMPS sends a *port-shutdown* response.

If the port already has a VLAN assignment, the VMPS provides one of these responses:

- If the VLAN in the database matches the current VLAN on the port, the VMPS sends an *success* response, allowing access to the host.
- If the VLAN in the database does not match the current VLAN on the port and active hosts exist on the port, the VMPS sends an *access-denied* or a *port-shutdown* response, depending on the secure mode of the VMPS.

If the switch receives an *access-denied* response from the VMPS, it continues to block traffic to and from the host MAC address. The switch continues to monitor the packets directed to the port and sends a query to the VMPS when it identifies a new host address. If the switch receives a *port-shutdown* response from the VMPS, it disables the port. The port must be manually re-enabled by using the CLI or SNMP.

Dynamic-Access Port VLAN Membership

A dynamic-access port can belong to only one VLAN with an ID from 1 to 4094. When the link comes up, the switch does not forward traffic to or from this port until the VMPS provides the VLAN assignment. The VMPS receives the source MAC address from the first packet of a new host connected to the dynamic-access port and attempts to match the MAC address to a VLAN in the VMPS database.

Note Only UNIs or ENIs can be dynamic-access ports.

If there is a match, the VMPS sends the VLAN number for that port. If the client switch was not previously configured, it uses the domain name from the first VTP packet it receives on its trunk port from the VMPS. If the client switch was previously configured, it includes its domain name in the query packet to the VMPS to obtain its VLAN number. The VMPS verifies that the domain name in the packet matches its own domain name before accepting the request and responds to the client with the assigned VLAN number for the client. If there is no match, the VMPS either denies the request or shuts down the port (depending on the VMPS secure mode setting).

Multiple hosts (MAC addresses) can be active on a dynamic-access port if they are all in the same VLAN; however, the VMPS shuts down a dynamic-access port if more than 20 hosts are active on the port.

If the link goes down on a dynamic-access port, the port returns to an isolated state and does not belong to a VLAN. Any hosts that come online through the port are checked again through the VQP with the VMPS before the port is assigned to a VLAN.

Dynamic-access ports can be used for direct host connections, or they can connect to a network. A maximum of 20 MAC addresses are allowed per port on the switch. A dynamic-access port can belong to only one VLAN at a time, but the VLAN can change over time, depending on the MAC addresses seen.

Prerequisites

- IP address of the switch acting as the primary VMPS
- IP connectivity to the VMPS for dynamic-access ports to work

Guidelines and Limitations

These guidelines and restrictions apply to dynamic-access port VLAN membership:

- You should configure the VMPS before you configure ports as dynamic-access ports.
- 802.1x ports cannot be configured as dynamic-access ports. If you try to enable 802.1x on a dynamic-access (VQP) port, an error message appears, and 802.1x is not enabled. If you try to change an 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
- Trunk ports cannot be dynamic-access ports, but you can enter the **switchport access vlan dynamic** interface configuration command for a trunk port. In this case, the switch retains the setting and applies it if the port is later configured as an access port.

  You must turn off trunking on the port before the dynamic-access setting takes effect.
- Dynamic-access ports cannot be monitor ports.
- Secure ports cannot be dynamic-access ports. You must disable port security on a port before it becomes dynamic.
- Private VLAN ports cannot be dynamic-access ports.
- Dynamic-access ports cannot be members of an EtherChannel group.
- Port channels cannot be configured as dynamic-access ports.

Default Settings

Feature	Default Setting
VMPS domain server	None
VMPS reconfirm interval	60 minutes
VMPS server retry count	3
Dynamic-access ports	None configured

Configuring the VMPS Client

You configure dynamic VLANs by using the VMPS (server). The switch can be a VMPS client; it cannot be a VMPS server.

Entering the IP Address of the VMPS

You must first enter the IP address of the server to configure the switch as a client.

BEFORE YOU BEGIN

Obtain the IP address of the VMPS.

Test for IP connectivity to the VMPS by pinging the IP address of the VMPS and verifying that you get a response.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vmps server** *ipaddress* **primary**	Enter the IP address of the switch acting as the primary VMPS server.
Step 3	**vmps server** *ipaddress*	(Optional) Enter the IP address of the switch acting as a secondary VMPS server. You can enter up to three secondary server addresses.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show vmps**	Verify your entries in the *VMPS Domain Server* field of the display.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to enter the IP addresses of the primary and secondary VMPS servers on the VMPS client:

```
Switch(config)# vmps server 172.20.26.150 primary
Switch(config)# vmps server 172.20.26.152
Switch(config)# exit
Switch# show vmps

VQP Client Status:
--------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.26.152
                    172.20.26.150 (primary, current
```

Configuring Dynamic-Access Ports on VMPS Clients

BEFORE YOU BEGIN

Caution Dynamic-access port VLAN membership is for end stations or hubs connected to end stations. Connecting dynamic-access ports to other switches can cause a loss of connectivity.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the switch port that is connected to the end station, and enter interface configuration mode. **Note** The port must be a UNI or an ENI.
Step 3	**no shutdown**	Enable the port.
Step 4	**port-type** {**uni** | **eni**}	Configure the port as a UNI or ENI.
Step 5	**switchport mode access**	Set the port to access mode.
Step 6	**switchport access vlan dynamic**	Configure the port as eligible for dynamic VLAN membership. The dynamic-access port must be connected to an end station.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Operational Mode* field of the display.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command. To reset the access mode to the default VLAN for the switch, use the **no switchport access vlan** interface configuration command.

EXAMPLE

This example shows how to configure a port as a dynamic-access port:

```
Switch(config)# interface GigabitEthernet1/1
Switch(config-if)# port-type uni
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan dynamic
Switch(config-if)# end
```

Reconfirming VLAN Memberships

A reconfirmation attempt can occur automatically when the reconfirmation interval expires, or you can force it by entering the **vmps reconfirm** privileged EXEC command. Follow this procedure to to confirm the dynamic-access port VLAN membership assignments that the switch has received from the VMPS.

BEFORE YOU BEGIN

Configure the switch as a VMPS client as described in the "Entering the IP Address of the VMPS" section on page 6-56.

DETAILED STEPS

	Command	Purpose
Step 1	**vmps reconfirm**	Reconfirm dynamic-access port VLAN membership.
Step 2	**show vmps**	Verify the dynamic VLAN reconfirmation status.

EXAMPLE

This example shows how to immediately send VQP queries to the VMPS:

```
Switch# vmps reconfirm
```

Changing the Reconfirmation Interval

VMPS clients periodically reconfirm the VLAN membership information received from the VMPS.You can set the number of minutes after which reconfirmation occurs.

BEFORE YOU BEGIN

Configure the switch as a VMPS client as described in the "Entering the IP Address of the VMPS" section on page 6-56.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vmps reconfirm** *minutes*	Enter the number of minutes between reconfirmations of the dynamic VLAN membership. The range is 1 to 120. The default is 60 minutes.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vmps**	Verify the dynamic VLAN reconfirmation status in the *Reconfirm Interval* field of the display.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no vmps reconfirm** global configuration command.

EXAMPLE

This example shows how to set the VQP client to reconfirm dynamic VLAN entries every 20 minutes:

```
Switch(config)# vmps reconfirm 20
```

Changing the Retry Count

Follow this procedure to change the number of times that the switch attempts to contact the VMPS before querying the next server.

BEFORE YOU BEGIN

Configure the switch as a VMPS client as described in the "Entering the IP Address of the VMPS" section on page 6-56.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vmps retry** *count*	Change the retry count. The retry range is 1 to 10; the default is 3.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vmps**	Verify your entry in the *Server Retry Count* field of the display.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no vmps retry** global configuration command.

EXAMPLE

This example shows how to set the retry count to 7:

```
Switch(config)# vmps retry 7
```

Verifying Configuration

You can display information about the VMPS by using the **show vmps** privileged EXEC command. The switch displays this information about the VMPS:

- VMPS VQP Version—the version of VQP used to communicate with the VMPS. The switch queries the VMPS that is using VQP Version 1.
- Reconfirm Interval—the number of minutes the switch waits before reconfirming the VLAN-to-MAC-address assignments.
- Server Retry Count—the number of times VQP resends a query to the VMPS. If no response is received after this many tries, the switch starts to query the secondary VMPS.
- VMPS domain server—the IP address of the configured VLAN membership policy servers. The switch sends queries to the one marked *current*. The one marked *primary* is the primary server.
- VMPS Action—the result of the most recent reconfirmation attempt. A reconfirmation attempt can occur automatically when the reconfirmation interval expires, or you can force it by entering the **vmps reconfirm** privileged EXEC command.

This is an example of output for the **show vmps** privileged EXEC command:

```
Switch# show vmps
VQP Client Status:
--------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
                    172.20.128.87

Reconfirmation status
---------------------
VMPS Action:         other
```

Troubleshooting Dynamic-Access Port VLAN Membership

The VMPS shuts down a dynamic-access port under these conditions:

- The VMPS is in secure mode, and it does not allow the host to connect to the port. The VMPS shuts down the port to prevent the host from connecting to the network.
- More than 20 active hosts reside on a dynamic-access port.

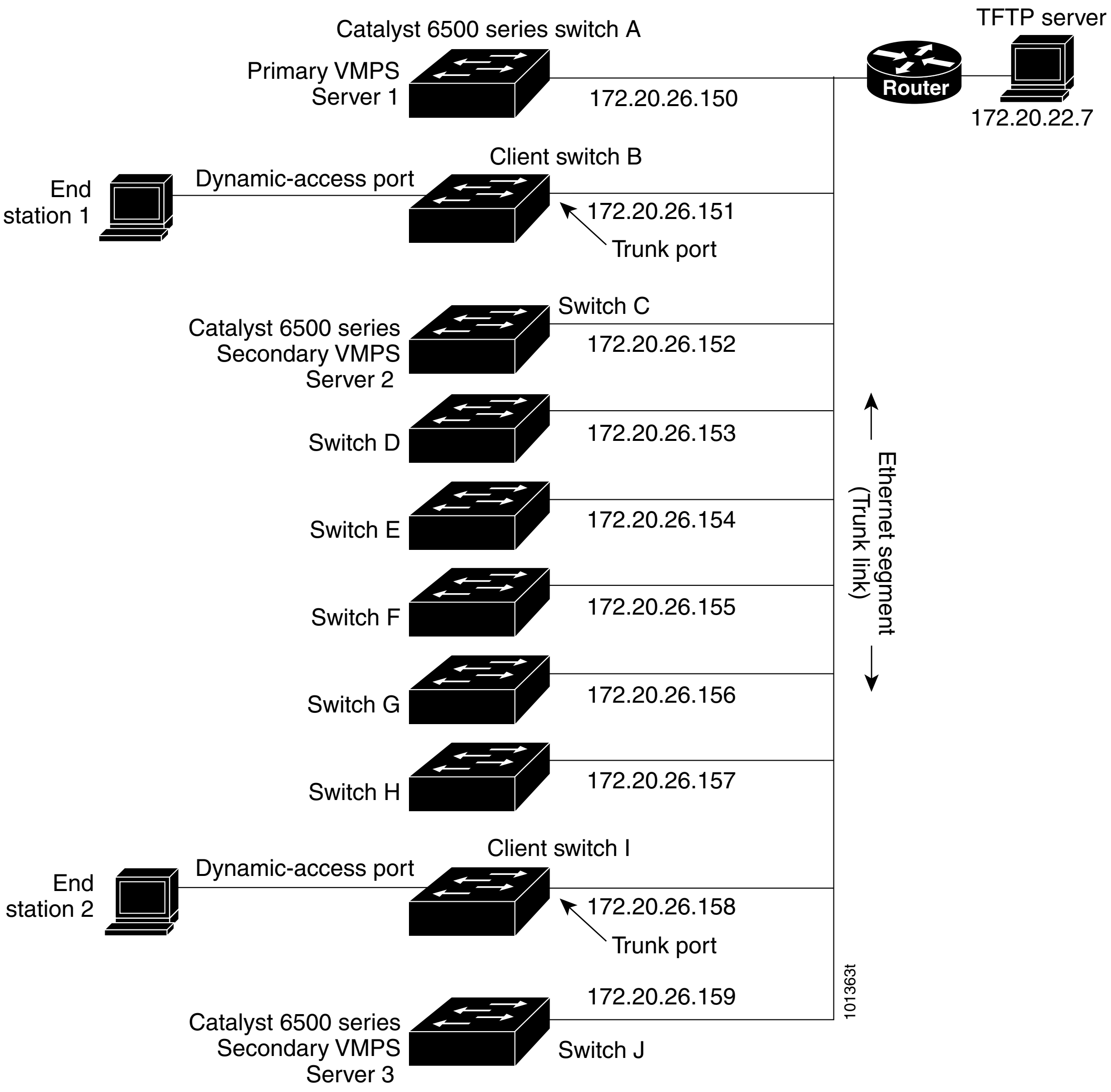
To disable and re-enable a disabled dynamic-access port, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

Configuration Example

Figure 6-1 shows a network with a VMPS server switch and VMPS client switches with dynamic-access ports. In this example, these assumptions apply:

- The VMPS server and the VMPS client are separate switches.
- The Catalyst 6500 series Switch A is the primary VMPS server.
- The Catalyst 6500 series Switch C and Switch J are secondary VMPS servers.
- End stations are connected to the clients, Switch B and Switch I.
- The database configuration file is stored on the TFTP server with the IP address 172.20.22.7.

Figure 6-1 Dynamic Port VLAN Membership Configuration



Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS Interface and Hardware Component Command Reference
- Catalyst 3750 Metro Switch Command Reference, Release 12.2(58)SE

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520 Switch	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

CHAPTER 7

Configuring Private VLANs

This chapter describes how to configure private VLANs on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*.

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 7-17.

This chapter includes the following sections:

- Information About Private VLANs, page 7-1
- Prerequisites, page 7-6
- Guidelines and Limitations, page 7-6
- Default Settings, page 7-9
- Configuring Private VLANs, page 7-9
- Verifying Configuration, page 7-15
- Configuration Example, page 7-16
- Related Documents, page 7-17
- Feature History, page 7-18

Information About Private VLANs

The private-VLAN feature addresses two problems that service providers face when using VLANs:

- Scalability: The switch supports up to 1005 active VLANs. If a service provider assigns one VLAN per customer, this limits the numbers of customers that the service provider can support.
- To enable IP routing, each VLAN is assigned a subnet address space or a block of addresses, which can waste the unused IP addresses and cause IP address management problems.

Using private VLANs addresses the scalability problem and provides IP address management benefits for service providers and Layer 2 security for customers.

These sections describe how private VLANs work:

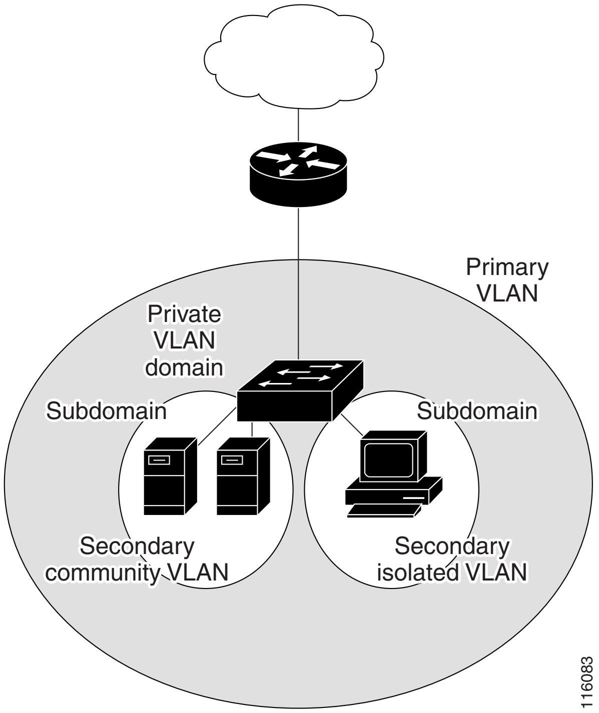
- Types of Private VLANs and Private-VLAN Ports, page 7-2
- IP Addressing Scheme with Private VLANs, page 7-4
- Private VLANs across Multiple Switches, page 7-4

- Private VLANs and Unicast, Broadcast, and Multicast Traffic, page 7-5
- Private VLANs and SVIs, page 7-6

Types of Private VLANs and Private-VLAN Ports

Private VLANs partition a regular VLAN domain into subdomains. A subdomain is represented by a pair of VLANs: a *primary* VLAN and a *secondary* VLAN. A private VLAN can have multiple VLAN pairs, one pair for each subdomain. All VLAN pairs in a private VLAN share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another. See Figure 7-1.

Figure 7-1 Private-VLAN Domain



There are two types of secondary VLANs:

- Isolated VLANs—Ports within an isolated VLAN cannot communicate with each other at the Layer 2 level.
- Community VLANs—Ports within a community VLAN can communicate with each other but cannot communicate with ports in other communities at the Layer 2 level. A community VLAN can include a combination of no more than eight user network interfaces (UNIs) and enhanced network interfaces (ENIs).

Private VLANs provide Layer 2 isolation between ports within the same private VLAN. Private-VLAN ports are access ports that are one of these types:

- Promiscuous—A promiscuous port belongs to the primary VLAN and can communicate with all interfaces, including the community and isolated host ports that belong to the secondary VLANs associated with the primary VLAN.

Note Promiscuous ports must be network node interfaces (NNIs). UNIs or ENIs cannot be configured as promiscuous ports.

- Isolated—An isolated port is a host port that belongs to an isolated secondary VLAN. It has complete Layer 2 separation from other ports within the same private VLAN, except for the promiscuous ports. Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports.
- Community—A community port is a host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with promiscuous ports. These interfaces are isolated at Layer 2 from all other interfaces in other communities and from isolated ports within their private VLAN. No more than eight UNIs and ENIs can be community ports in the same community VLAN.

Note Trunk ports carry traffic from regular VLANs and also from primary, isolated, and community VLANs.

Primary and secondary VLANs have these characteristics:

- Primary VLAN—A private VLAN has only one primary VLAN. Every port in a private VLAN is a member of the primary VLAN. The primary VLAN carries unidirectional traffic downstream from the promiscuous ports to the (isolated and community) host ports and to other promiscuous ports.
- Isolated VLAN —A private VLAN has only one isolated VLAN. An isolated VLAN is a secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports and the gateway.
- Community VLAN—A community VLAN is a secondary VLAN that carries upstream traffic from the community ports to the promiscuous port gateways and to other host ports in the same community. You can configure multiple community VLANs in a private VLAN. Each community VLAN can include a combination of no more than eight UNIs and ENIs.

Note The switch also supports UNI-ENI isolated VLANs and UNI-ENI community VLANs. When a VLAN is created, it is by default a UNI-ENI isolated VLAN. Traffic is not switched among UNIs and ENIs on a switch that belong to a UNI-ENI isolated VLAN. For more information on UNI-ENI VLANs, see Chapter 3, "Configuring VLANs."

A promiscuous port can serve only one primary VLAN, one isolated VLAN, and multiple community VLANs. Layer 3 gateways are typically connected to the switch through a promiscuous port. With a promiscuous port, you can connect a wide range of devices as access points to a private VLAN. For example, you can use a promiscuous port to monitor or back up all the private-VLAN servers from an administration workstation.

In a switched environment, you can assign an individual private VLAN and associated IP subnet to each individual or common group of end stations. The end stations need to communicate only with a default gateway to communicate outside the private VLAN.

You can use private VLANs to control access to end stations in these ways:

- Configure selected interfaces connected to end stations as isolated ports to prevent any communication at Layer 2. For example, if the end stations are servers, this configuration prevents Layer 2 communication between the servers.
- Configure NNIs connected to default gateways and selected end stations (for example, backup servers) as promiscuous ports to allow all end stations access to a default gateway.

You can extend private VLANs across multiple devices by trunking the primary, isolated, and community VLANs to other devices that support private VLANs. To maintain the security of your private-VLAN configuration and to avoid other use of the VLANs configured as private VLANs, configure private VLANs on all intermediate devices, including devices that have no private-VLAN ports.

IP Addressing Scheme with Private VLANs

Assigning a separate VLAN to each customer creates an inefficient IP addressing scheme:

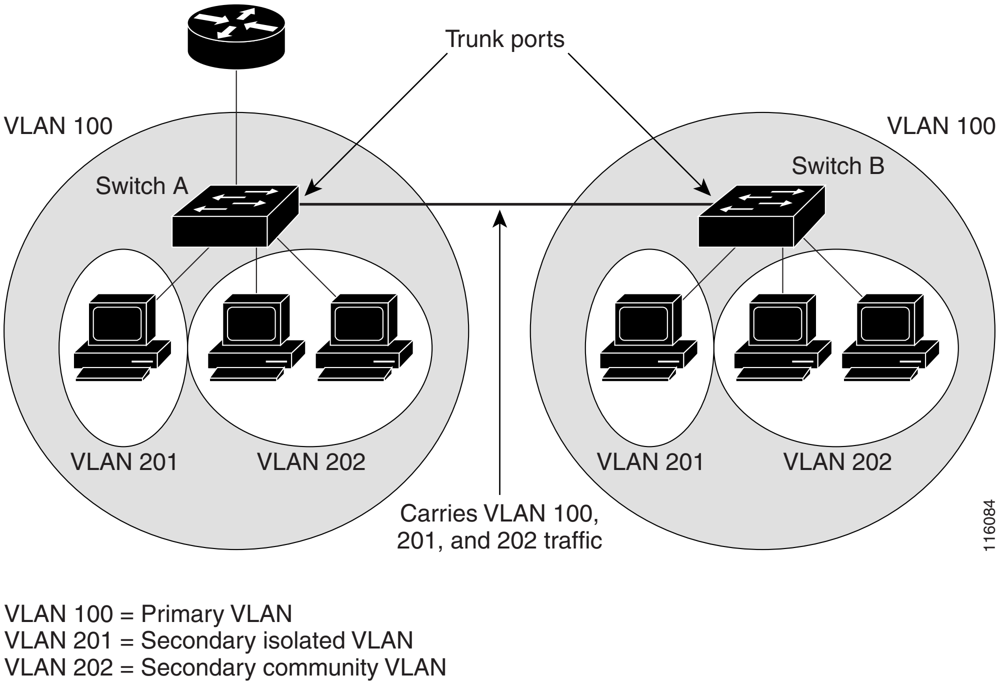
- Assigning a block of addresses to a customer VLAN can result in unused IP addresses.
- If the number of devices in the VLAN increases, the number of assigned address might not be large enough to accommodate them.

These problems are reduced by using private VLANs, where all members in the private VLAN share a common address space, which is allocated to the primary VLAN. Hosts are connected to secondary VLANs, and the DHCP server assigns them IP addresses from the block of addresses allocated to the primary VLAN. Subsequent IP addresses can be assigned to customer devices in different secondary VLANs, but in the same primary VLAN. When new devices are added, the DHCP server assigns them the next available address from a large pool of subnet addresses.

Private VLANs across Multiple Switches

As with regular VLANs, private VLANs can span multiple switches. A trunk port carries the primary VLAN and secondary VLANs to a neighboring switch. The trunk port treats the private VLAN as any other VLAN. A feature of private VLANs across multiple switches is that traffic from an isolated port in switch A does not reach an isolated port on Switch B. See Figure 7-2.

Figure 7-2 Private VLANs across Switches


Trunk ports
VLAN 100
VLAN 100
Switch A
Switch B
VLAN 201
VLAN 202
VLAN 201
VLAN 202
Carries VLAN 100, 201, and 202 traffic
116084
VLAN 100 = Primary VLAN
VLAN 201 = Secondary isolated VLAN
VLAN 202 = Secondary community VLAN

You must manually configure private VLANs on all switches in the Layer 2 network. If you do not configure the primary and secondary VLAN associations in some switches in the network, the Layer 2 databases in these switches are not merged. This can result in unnecessary flooding of private-VLAN traffic on those switches.

Private VLANs and Unicast, Broadcast, and Multicast Traffic

In regular VLANs, devices in the same VLAN can communicate with each other at the Layer 2 level, but devices connected to interfaces in different VLANs must communicate at the Layer 3 level. In private VLANs, the promiscuous ports are members of the primary VLAN, while the host ports belong to secondary VLANs. Because the secondary VLAN is associated to the primary VLAN, members of the these VLANs can communicate with each other at the Layer 2 level.

In a regular VLAN, broadcasts are forwarded to all ports in that VLAN. Private-VLAN broadcast forwarding depends on the port sending the broadcast:

- An isolated port sends a broadcast only to the promiscuous ports or trunk ports.
- A community port sends a broadcast to all promiscuous ports, trunk ports, and ports in the same community VLAN.
- A promiscuous port (only NNI) sends a broadcast to all ports in the private VLAN (other promiscuous ports, trunk ports, isolated ports, and community ports).

Multicast traffic is routed or bridged across private-VLAN boundaries and within a single community VLAN. Multicast traffic is not forwarded between ports in the same isolated VLAN or between ports in different secondary VLANs.

Private VLANs and SVIs

In a Layer 3 switch (a switch running the IP services image), a switch virtual interface (SVI) represents the Layer 3 interface of a VLAN. Layer 3 devices communicate with a private VLAN only through the primary VLAN and not through secondary VLANs. Configure Layer 3 VLAN interfaces only for primary VLANs. You cannot configure Layer 3 VLAN interfaces for secondary VLANs. SVIs for secondary VLANs are inactive while the VLAN is configured as a secondary VLAN.

- If you try to configure a VLAN with an active SVI as a secondary VLAN, the configuration is not allowed until you disable the SVI.
- If you try to create an SVI on a VLAN that is configured as a secondary VLAN and the secondary VLAN is already mapped at Layer 3, the SVI is not created, and an error is returned. If the SVI is not mapped at Layer 3, the SVI is created, but it is automatically shut down.

When the primary VLAN is associated with and mapped to the secondary VLAN, any configuration on the primary VLAN is propagated to the secondary VLAN SVIs. For example, if you assign an IP subnet to the primary VLAN SVI, this subnet is the IP subnet address of the entire private VLAN.

Prerequisites

- Be familiar with the information in the "Information About Private VLANs" section on page 7-1 and "Guidelines and Limitations" section on page 7-6.
- Ensure that your network strategy and planning for your network are complete.

Guidelines and Limitations

Secondary and Primary VLAN Configuration

Follow these guidelines when configuring private VLANs:

- You use VLAN configuration mode to configure private VLANs. For more information about VLAN configuration, see Chapter 3, "Configuring VLANs."
- You must configure private VLANs on each device where you want private-VLAN ports.
- A private VLAN cannot be a UNI-ENI VLAN.
  - To change a UNI-ENI isolated VLAN (the default) to a private VLAN, enter the **private-vlan** VLAN configuration command; this overwrites the default isolated VLAN configuration.
  - To change a UNI-ENI community VLAN to a private VLAN, you must first enter the **no uni-vlan** VLAN configuration command to return to the default UNI isolated VLAN configuration.
- You cannot configure VLAN 1 or VLANs 1002 to 1005 as primary or secondary VLANs. Extended VLANs (VLAN IDs 1006 to 4094) can belong to private VLANs
- A primary VLAN can have one isolated VLAN and multiple community VLANs associated with it. An isolated or community VLAN can have only one primary VLAN associated with it.
- Although a private VLAN contains more than one VLAN, only one Spanning Tree Protocol (STP) instance runs for the entire private VLAN. When a secondary VLAN is associated with the primary VLAN, the STP parameters of the primary VLAN are propagated to the secondary VLAN.

- You can enable DHCP snooping on private VLANs. When you enable DHCP snooping on the primary VLAN, it is propagated to the secondary VLANs. If you configure DHCP on a secondary VLAN, the configuration does not take effect if the primary VLAN is already configured.
- If you enable IP source guard on private-VLAN ports, you must enable DHCP snooping on the primary VLAN.
- You can apply different quality of service (QoS) configurations to primary, isolated, and community VLANs.
- When the switch is running the IP services image, for sticky ARP:
  - Sticky ARP entries are those learned on SVIs and Layer 3 interfaces. The entries do not age out.
  - The **ip sticky-arp** global configuration command is supported only on SVIs belonging to private VLANs.
  - The **ip sticky-arp** interface configuration command is only supported on

    Layer 3 interfaces

    SVIs belonging to normal VLANs

    SVIs belonging to private VLANs

  For more information about using the **ip sticky-arp** *global* configuration and the **ip sticky-arp** *interface* configuration commands, see the *Cisco IOS IP Addressing Services Command Reference*.
- You can configure VLAN maps on primary and secondary VLANs (see the “Configuring VLAN Maps” section of the “Configuring Network Security with ACLs” chapter in the *Security Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*). However, we recommend that you configure the same VLAN maps on private-VLAN primary and secondary VLANs.
- When a frame is forwarded through Layer 2 within a private VLAN, the same VLAN map is applied at the receiving and sending sides. When a frame is routed from inside a private VLAN to an external port, the private-VLAN map is applied at the receiving side.
  - For frames going upstream from a host port to a promiscuous port, the VLAN map configured on the secondary VLAN is applied.
  - For frames going downstream from a promiscuous port to a host port, the VLAN map configured on the primary VLAN is applied.

  To filter out specific IP traffic for a private VLAN, you should apply the VLAN map to both the primary and secondary VLANs.
- If the switch is running the IP services image, you can apply router ACLs only on the primary-VLAN SVIs. The ACL is applied to both primary and secondary VLAN Layer 3 traffic.
- Although private VLANs provide host isolation at Layer 2, hosts can communicate with each other at Layer 3.
- Private VLANs support these Switched Port Analyzer (SPAN) features:
  - You can configure a private-VLAN port as a SPAN source port.
  - You can use VLAN-based SPAN (VSPAN) on primary, isolated, and community VLANs or use SPAN on only one VLAN to separately monitor sent or received traffic.

Private-VLAN Port Configuration

Follow these guidelines when configuring private-VLAN ports:

- Promiscuous ports must be NNIs; UNIs and ENIs cannot be configured as promiscuous ports.

- Use only the private-VLAN configuration commands to assign ports to primary, isolated, or community VLANs. Layer 2 access ports assigned to the VLANs that you configure as primary, isolated, or community VLANs are inactive while the VLAN is part of the private-VLAN configuration. Layer 2 trunk interfaces remain in the STP forwarding state.
- Do not configure NNI ports that belong to a Port Aggregation Protocol (PAgP) or Link Aggregation Control Protocol (LACP) EtherChannel as private-VLAN ports. While a port is part of the private-VLAN configuration, any EtherChannel configuration for it is inactive.
- Enable Port Fast and BPDU guard on NNI isolated and community host ports to prevent STP loops due to misconfigurations and to speed up STP convergence (see Chapter 13, "Configuring Optional Spanning-Tree Features"). When enabled, STP applies the BPDU guard feature to all Port Fast-configured Layer 2 LAN ports. Do not enable Port Fast and BPDU guard on promiscuous ports.
- If you delete a VLAN used in the private-VLAN configuration, the private-VLAN ports associated with the VLAN become inactive.
- Private-VLAN ports can be on different network devices if the devices are trunk-connected and the primary and secondary VLANs have not been removed from the trunk.
- A community private VLAN can include no more than eight UNIs and ENIs. If you try to add more than eight, the configuration is not allowed. If you try to configure a VLAN that includes a combination of more than eight UNIs and ENIs as a community private VLAN, the configuration is not allowed.

Limitations with Other Features

When configuring private VLANs, remember these limitations with other features:

Note In some cases, the configuration is accepted with no error messages, but the commands have no effect.

- When IGMP snooping is enabled on the switch (the default), the switch supports no more than 20 private-VLAN domains.
- A private VLAN cannot be a UNI-ENI isolated or UNI-ENI community VLAN. For more information about UNI-ENI VLANs, see Chapter 3, "Configuring VLANs."
- Do not configure a remote SPAN (RSPAN) VLAN as a private-VLAN primary or secondary VLAN. For more information about SPAN, see the "Configuring SPAN and RSPAN" chapter in the *System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.
- Do not configure private-VLAN ports on interfaces configured for these other features:
  - dynamic-access port VLAN membership
  - PAgP (only NNIs or ENIs)
  - LACP (only NNIs or ENIs)
  - Multicast VLAN Registration (MVR)
- You can configure 802.1x port-based authentication on a private-VLAN port, but do not configure IEEE 802.1x with port security on private-VLAN ports.

- A private-VLAN host or promiscuous port cannot be a SPAN destination port. If you configure a SPAN destination port as a private-VLAN port, the port becomes inactive.
- If you configure a static MAC address on a promiscuous port in the primary VLAN, you must add the same static address to all associated secondary VLANs. If you configure a static MAC address on a host port in a secondary VLAN, you must add the same static MAC address to the associated primary VLAN. When you delete a static MAC address from a private-VLAN port, you must remove all instances of the configured MAC address from the private VLAN.

Note Dynamic MAC addresses learned in one VLAN of a private VLAN are replicated in the associated VLANs. For example, a MAC address learned in a secondary VLAN is replicated in the primary VLAN. When the original dynamic MAC address is deleted or aged out, the replicated addresses are removed from the MAC address table.

- Configure Layer 3 VLAN interfaces only for primary VLANs.

Default Settings

No private VLANs are configured. Newly created VLANs are UNI-ENI isolated VLANs.

Configuring Private VLANs

This section includes the following topics:

- Tasks for Configuring Private VLANs, page 7-9
- Configuring and Associating VLANs in a Private VLAN, page 7-10
- Configuring a Layer 2 Interface as a Private-VLAN Host Port, page 7-12
- Configuring a Layer 2 Interface as a Private-VLAN Promiscuous Port, page 7-13
- Mapping Secondary VLANs to a Primary VLAN Layer 3 VLAN Interface, page 7-14

Tasks for Configuring Private VLANs

To configure a private VLAN, follow these steps:

Step 1 Create the primary and secondary VLANs and associate them. See the "Configuring and Associating VLANs in a Private VLAN" section on page 7-10.

Note If the VLAN is not created already, the private-VLAN configuration process creates it.

Step 2 Configure interfaces to be isolated or community host ports, and assign VLAN membership to the host port. See the "Configuring a Layer 2 Interface as a Private-VLAN Host Port" section on page 7-12.

Step 3 Configure NNIs as promiscuous ports, and map the promiscuous ports to the primary-secondary VLAN pair. See the "Configuring a Layer 2 Interface as a Private-VLAN Promiscuous Port" section on page 7-13.

Step 4 If inter-VLAN routing will be used, configure the primary SVI, and map secondary VLANs to the primary. See the "Mapping Secondary VLANs to a Primary VLAN Layer 3 VLAN Interface" section on page 7-14.

Step 5 Verify private-VLAN configuration.

Configuring and Associating VLANs in a Private VLAN

Create the primary and secondary VLANs and associate them.

BEFORE YOU BEGIN

When you associate secondary VLANs with a primary VLAN, note this syntax information:

- The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs.
- The *secondary_vlan_list* parameter can contain multiple community VLAN IDs but only one isolated VLAN ID.
- Enter a *secondary_vlan_list,* or use the **add** keyword with a *secondary_vlan_list* to associate secondary VLANs with a primary VLAN.
- Use the **remove** keyword with a *secondary_vlan_list* to clear the association between secondary VLANs and a primary VLAN.
- The **private-vlan association** VLAN configuration command does not take effect until you exit VLAN configuration mode.

DETAILED STEPS

Note The **private-vlan** commands do not take effect until you exit VLAN configuration mode.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vlan** *vlan-id*	Enter VLAN configuration mode and designate or create a VLAN that will be the primary VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094. **Note** If the VLAN has been configured as a UNI-ENI community VLAN, you must enter the **no uni-vlan** VLAN configuration command before configuring a private VLAN.
Step 3	**private-vlan primary**	Designate the VLAN as the primary VLAN.
Step 4	**exit**	Return to global configuration mode.
Step 5	**vlan** *vlan-id*	(Optional) Enter VLAN configuration mode and designate or create a VLAN that will be an isolated VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094.
Step 6	**private-vlan isolated**	Designate the VLAN as an isolated VLAN.

	Command	Purpose
Step 7	**exit**	Return to global configuration mode.
Step 8	**vlan** *vlan-id*	(Optional) Enter VLAN configuration mode and designate or create a VLAN that will be a community VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094. **Note** If the VLAN has been configured as a UNI-ENI community VLAN, you must enter the **no uni-vlan** VLAN configuration command before configuring a private VLAN.
Step 9	**private-vlan community**	Designate the VLAN as a community VLAN.
Step 10	**exit**	Return to global configuration mode.
Step 11	**vlan** *vlan-id*	Enter VLAN configuration mode for the primary VLAN designated in Step 3.
Step 12	**private-vlan association** [**add** | **remove**] *secondary_vlan_list*	Associate the secondary VLANs with the primary VLAN.
Step 13	**end**	Return to privileged EXEC mode.
Step 14	**show vlan private-vlan** [**type**] or **show interfaces status**	Verify the configuration.
Step 15	**copy running-config startup config**	(Optional) Save your entries in the switch startup configuration file.

EXAMPLE

This example shows how to configure VLAN 20 as a primary VLAN, VLAN 501 as an isolated VLAN, and VLANs 502 and 503 as community VLANs, to associate them in a private VLAN, and to verify the configuration. It assumes that VLANs 502 and 503 have previously been configured as UNI-ENI community VLANs:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# no uni-vlan
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# no uni-vlan
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-503
Switch(config-vlan)# end
Switch(config)# show vlan private vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
20      501       isolated
20      502       community
```

```
20      503      community
20      504      non-operational
```

Configuring a Layer 2 Interface as a Private-VLAN Host Port

Configure interfaces to be isolated or community host ports, and assign VLAN membership to the host port.

Note Isolated and community VLANs are both secondary VLANs.

BEFORE YOU BEGIN

Perform the "Configuring and Associating VLANs in a Private VLAN" procedure on page 7-10.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode for the Layer 2 interface to be configured.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	**switchport mode private-vlan host**	Configure the Layer 2 port as a private-VLAN host port.
Step 5	**switchport private-vlan host-association** *primary_vlan_id secondary_vlan_id*	Associate the Layer 2 port with a private VLAN.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show interfaces** [*interface-id*] **switchport**	Verify the configuration.
Step 8	**copy running-config startup config**	(Optional) Save your entries in the switch startup configuration file.

EXAMPLE

This example shows how to configure an interface as a private-VLAN host port, associate it with a private-VLAN pair, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/22
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
Switch(config-if)# end
Switch# show interfaces fastethernet0/22 switchport
Name: Fa0/22
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
```

```
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Administrative private-vlan host-association: 20 501
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
20 501
<output truncated>
```

Configuring a Layer 2 Interface as a Private-VLAN Promiscuous Port

Follow this procedure to configure a Layer 2 interface as a private-VLAN promiscuous port and map it to primary and secondary VLANs. You can configure only NNIs as promiscuous ports.

Note Isolated and community VLANs are both secondary VLANs.

BEFORE YOU BEGIN

- Perform the "Configuring a Layer 2 Interface as a Private-VLAN Host Port" procedure on page 7-12.
- When you configure a Layer 2 interface as a private-VLAN promiscuous port, note this syntax information:
  - The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs.
  - Enter a *secondary_vlan_list*, or use the **add** keyword with a *secondary_vlan_list* to map the secondary VLANs to the private-VLAN promiscuous port.
  - Use the **remove** keyword with a *secondary_vlan_list* to clear the mapping between secondary VLANs and the private-VLAN promiscuous port.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode for the Layer 2 interface to be configured. The interface must be an NNI. **Note** If the interface is a UNI or ENI, you must enter the **port-type nni** interface configuration command before configuring it as a promiscuous port.

	Command	Purpose
Step 3	**switchport mode private-vlan promiscuous**	Configure the Layer 2 NNI port as a private-VLAN promiscuous port.
Step 4	**switchport private-vlan mapping** *primary_vlan_id* {**add** | **remove**} *secondary_vlan_list*	Map the private-VLAN promiscuous port to a primary VLAN and to selected secondary VLANs.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show interfaces** [*interface-id*] **switchport**	Verify the configuration.
Step 7	**copy running-config startup config**	(Optional) Save your entries in the switch startup configuration file.

EXAMPLE

This example shows how to configure an NNI as a private-VLAN promiscuous port and map it to a private VLAN. The interface is a member of primary VLAN 20 and secondary VLANs 501 to 503 are mapped to it.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
Switch(config-if)# end
```

Use the **show vlan private-vlan** or the **show interface status** privileged EXEC command to display primary and secondary VLANs and private-VLAN ports on the switch.

Mapping Secondary VLANs to a Primary VLAN Layer 3 VLAN Interface

If the switch is running the IP services image and the private VLAN will be used for inter-VLAN routing, you configure an SVI for the primary VLAN and map secondary VLANs to the SVI.

Note Isolated and community VLANs are both secondary VLANs.

BEFORE YOU BEGIN

- Perform the "Configuring a Layer 2 Interface as a Private-VLAN Promiscuous Port" procedure on page 7-13.
- When you map secondary VLANs to the Layer 3 VLAN interface of a primary VLAN, note this syntax information:
  - The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs.
  - Enter a *secondary_vlan_list,* or use the **add** keyword with a *secondary_vlan_list* to map the secondary VLANs to the primary VLAN.
  - Use the **remove** keyword with a *secondary_vlan_list* to clear the mapping between secondary VLANs and the primary VLAN.

Note The **private-vlan mapping** interface configuration command only affects private-VLAN traffic that is switched through Layer 3.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface vlan** *primary_vlan_id*	Enter interface configuration mode for the primary VLAN, and configure the VLAN as an SVI. The VLAN ID range is 2 to 1001 and 1006 to 4094.
Step 3	**private-vlan mapping** [**add** | **remove**] *secondary_vlan_list*	Map the secondary VLANs to the Layer 3 VLAN interface of a primary VLAN to allow Layer 3 switching of private-VLAN incoming traffic.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interface private-vlan mapping**	Verify the configuration.
Step 6	**copy running-config startup config**	(Optional) Save your entries in the switch startup configuration file.

EXAMPLE

This example shows how to map the interfaces of VLANs 501 and 502 to primary VLAN 10, which permits routing of secondary VLAN incoming traffic from private VLANs 501 to 502:

```
Switch# configure terminal
Switch(config)# interface vlan 10
Switch(config-if)# private-vlan mapping 501-502
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan10    501            isolated
vlan10    502            community
```

Verifying Configuration

Command	Purpose
show interfaces status	Display the status of interfaces, including the VLANs to which they belong.
show vlan private-vlan [**type**]	Display the private-VLAN information for the switch.
show interface switchport	Display the private-VLAN configuration on interfaces.
show interface private-vlan mapping	Display information about the private-VLAN mapping for VLAN interfaces.

Configuration Example

This example shows how to configure VLAN 20 as a primary VLAN, VLAN 501 as an isolated VLAN, and VLANs 502 and 503 as community VLANs, to associate them in a private VLAN, and to verify the configuration. It assumes that VLANs 502 and 503 have previously been configured as UNI-ENI community VLANs:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# no uni-vlan
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# no uni-vlan
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-503
Switch(config-vlan)# end
Switch(config)# show vlan private vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
20      501       isolated
20      502       community
20      503       community
20      504       non-operational
```

This example shows how to configure an interface as a private-VLAN host port, associate it with a private-VLAN pair, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/22
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
Switch(config-if)# end
Switch# show interfaces fastethernet0/22 switchport
Name: Fa0/22
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Administrative private-vlan host-association: 20 501
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
20 501
```

```
<output truncated>
```

This example shows how to configure an NNI as a private-VLAN promiscuous port and map it to a private VLAN. The interface is a member of primary VLAN 20 and secondary VLANs 501 to 503 are mapped to it.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
Switch(config-if)# end
```

This example shows how to map the interfaces of VLANs 501 and 502 to primary VLAN 10, which permits routing of secondary VLAN incoming traffic from private VLANs 501 to 502:

```
Switch# configure terminal
Switch(config)# interface vlan 10
Switch(config-if)# private-vlan mapping 501-502
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan10    501            isolated
vlan10    502            community
```

Use the **show vlan private-vlan** or the **show interface status** privileged EXEC command to display primary and secondary VLANs and private-VLAN ports on the switch.

```
Switch(config)# show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
10      501       isolated          Fa0/1, Gi0/1, Gi0/2
10      502       community         Fa0/11, Fa0/12, Gi0/1
10      503       non-operational
```

Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS LAN Switching Command Reference
- Cisco IOS Interface and Hardware Component Command Reference
- Cisco IOS IP Addressing Services Command Reference
- Security Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches
- System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520 Switch	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

CHAPTER 8

Configuring IEEE 802.1Q Tunneling

This chapter describes how to configure IEEE 802.1Q tunneling on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*.

Virtual private networks (VPNs) provide enterprise-scale connectivity on a shared infrastructure, often Ethernet-based, with the same security, prioritization, reliability, and manageability requirements of private networks. Tunneling is a feature designed for service providers who carry traffic of multiple customers across their networks and are required to maintain the VLAN and Layer 2 protocol configurations of each customer without impacting the traffic of other customers. The switch supports IEEE 802.1Q tunneling and Layer 2 protocol tunneling; Layer 2 protocol tunneling is described in Chapter 10, "Configuring Layer 2 Protocol Tunneling."

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 8-8.

This chapter includes the following sections:

- Information About 802.1Q Tunneling, page 8-1
- Prerequisites, page 8-4
- Guidelines and Limitations, page 8-4
- Default Settings, page 8-6
- Configuring an 802.1Q Tunneling Port, page 8-6
- Verifying Configuration, page 8-8
- Related Documents, page 8-8
- Feature History, page 8-8

Information About 802.1Q Tunneling

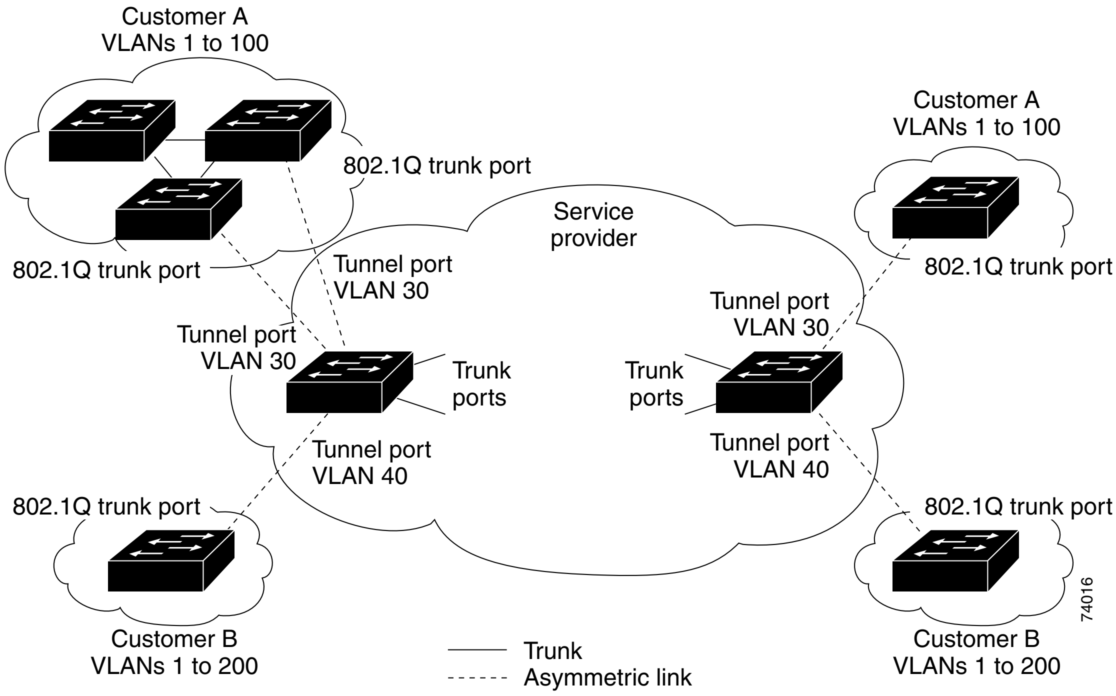
Business customers of service providers often have specific requirements for VLAN IDs and the number of VLANs to be supported. The VLAN ranges required by different customers in the same service-provider network might overlap, and traffic of customers through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations and could easily exceed the VLAN limit (4096) of the 802.1Q specification.

Using the 802.1Q tunneling (QinQ) feature, service providers can use a single VLAN to support customers who have multiple VLANs. Customer VLAN IDs (C-VLANs) are preserved, and traffic from different customers is segregated within the service-provider network, even when they appear to be in the same VLAN. Using 802.1Q tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy and retagging the tagged packets. A port configured to support 802.1Q tunneling is called a *tunnel port*. When you configure tunneling, you assign a tunnel port to a VLAN ID that is dedicated to tunneling. Each customer requires a separate service-provider VLAN ID (S-VLAN), but that VLAN ID supports all of the customer's VLANs. Configuring 802.1Q tunneling on a tunnel port is referred to as *traditional QinQ*.

Customer traffic tagged in the normal way with appropriate VLAN IDs comes from an 802.1Q trunk port on the customer device and into a tunnel port on the service-provider edge switch. The link between the customer device and the edge switch is asymmetric because one end is configured as an 802.1Q trunk port, and the other end is configured as a tunnel port. You assign the tunnel port interface to an access VLAN ID that is unique to each customer. See Figure 8-1.

Note By default, VLANs configured on the switch are user network interface-enhanced network interface (UNI-ENI) isolated VLANs. In a UNI-ENI isolated VLAN, 802.1Q tunneled access ports on the switch are isolated from each other. If you use the **uni-vlan community** VLAN configuration command to change a VLAN to a UNI-ENI community VLAN, local switching occurs between these ports. For more information about UNI-ENI VLANs, see Chapter 3, "Configuring VLANs."

Figure 8-1 802.1Q Tunnel Ports in a Service-Provider Network

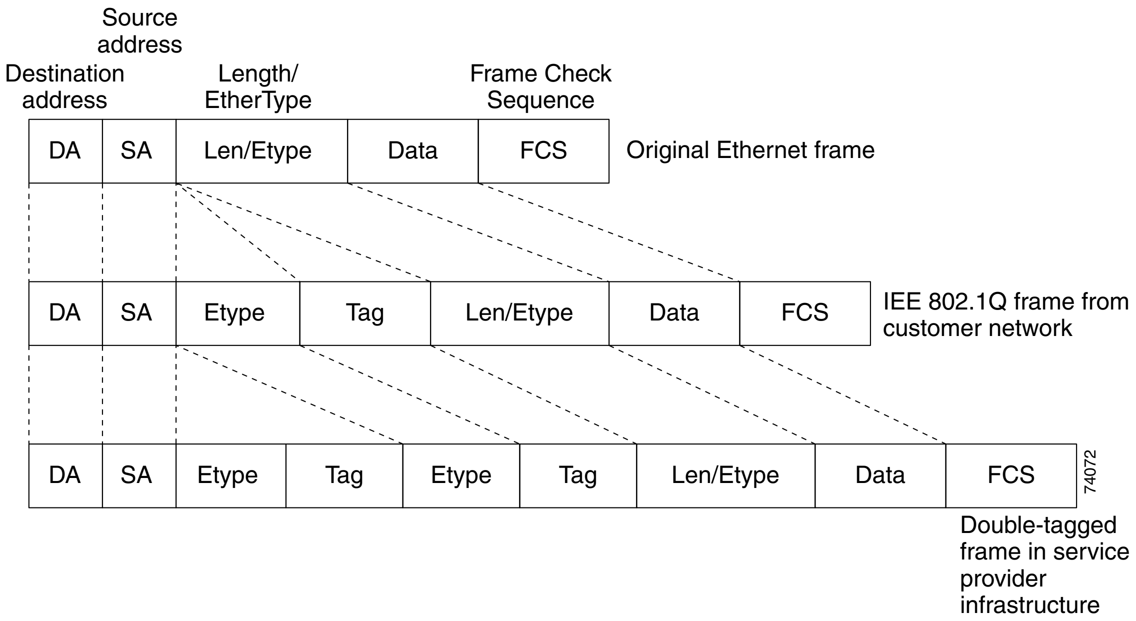


Packets coming from the customer trunk port into the tunnel port on the service-provider edge switch are normally 802.1Q-tagged with the appropriate VLAN ID. The tagged packets remain intact inside the switch and when they exit the trunk port into the service-provider network, they are encapsulated with another layer of an 802.1Q tag (called the *metro tag*) that contains the VLAN ID that is unique to the customer. The original customer 802.1Q tag is preserved in the encapsulated packet. Therefore, packets entering the service-provider network are double-tagged, with the outer (metro) tag containing the customer's access VLAN ID, and the inner VLAN ID being that of the incoming traffic.

When the double-tagged packet enters another trunk port in a service-provider core switch, the outer tag is stripped as the switch processes the packet. When the packet exits another trunk port on the same core switch, the same metro tag is again added to the packet. Figure 8-2 shows the tag structures of the double-tagged packets.

Note Remove the Layer 2 protocol configuration from a trunk port because incoming encapsulated packets change that trunk port to error disabled. The outgoing encapsulated VTP (CDP and STP) packets are dropped on that trunk.

Figure 8-2 Original (Normal), 802.1Q, and Double-Tagged Ethernet Packet Formats



When the packet enters the trunk port of the service-provider egress switch, the outer tag is again stripped as the switch internally processes the packet. However, the metro tag is not added when the packet is sent out the tunnel port on the edge switch into the customer network. The packet is sent as a normal 802.1Q-tagged frame to preserve the original VLAN numbers in the customer network.

In Figure 8-1, Customer A was assigned VLAN 30, and Customer B was assigned VLAN 40. Packets entering the edge switch tunnel ports with 802.1Q tags are double-tagged when they enter the service-provider network, with the outer tag containing VLAN ID 30 or 40, appropriately, and the inner tag containing the original VLAN number, for example, VLAN 100. Even if both Customers A and B have VLAN 100 in their networks, the traffic remains segregated within the service-provider network because the outer tag is different. Each customer controls its own VLAN numbering space, which is independent of the VLAN numbering space used by other customers and the VLAN numbering space used by the service-provider network.

At the outbound tunnel port, the original VLAN numbers on the customer's network are recovered. It is possible to have multiple levels of tunneling and tagging, but the switch supports only one level in this release.

If traffic coming from a customer network is not tagged (native VLAN frames), these packets are bridged or routed as normal packets. All packets entering the service-provider network through a tunnel port on an edge switch are treated as untagged packets, whether they are untagged or already tagged with 802.1Q headers. The packets are encapsulated with the metro tag VLAN ID (set to the access VLAN of the tunnel port) when they are sent through the service-provider network on an 802.1Q trunk port. The priority field on the metro tag is set to the interface class of service (CoS) priority configured on the tunnel port. (The default is zero if none is configured.)

Prerequisites

- Be familiar with the information in the "Information About 802.1Q Tunneling" section on page 8-1 and "Guidelines and Limitations" section on page 8-4.
- Ensure that your network strategy and planning for your network are complete.

Guidelines and Limitations

When you configure 802.1Q tunneling, you should always use an asymmetrical link between the customer device and the edge switch, with the customer device port configured as an 802.1Q trunk port and the edge switch port configured as a tunnel port.

Assign tunnel ports only to VLANs that are used for tunneling.

Configuration requirements for native VLANs, maximum transmission units (MTUs), and 802.1Q tunneling interactions with other features are explained in the next sections.

Native VLANs

When configuring 802.1Q tunneling on an edge switch, you must use 802.1Q trunk ports for sending packets into the service-provider network. However, packets going through the core of the service-provider network can be carried through 802.1Q trunks, ISL trunks, or nontrunking links. When 802.1Q trunks are used in these core switches, the native VLANs of the 802.1Q trunks must not match any native VLAN of the nontrunking (tunneling) port on the same switch because traffic on the native VLAN would not be tagged on the 802.1Q sending trunk port.

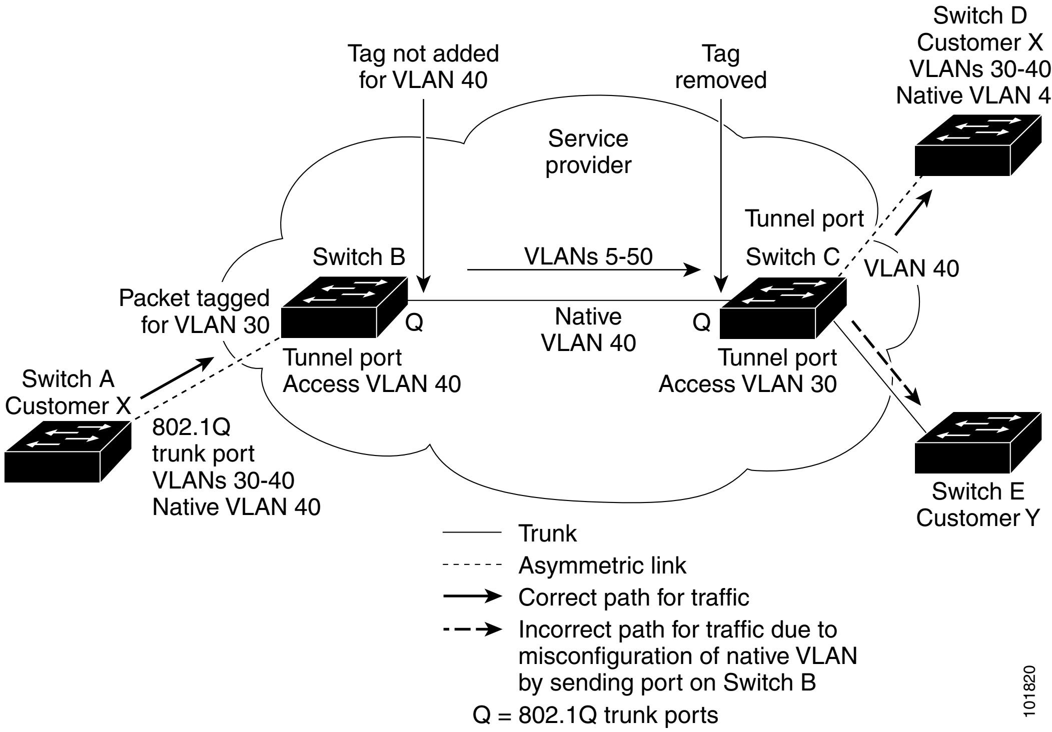
See Figure 8-3. VLAN 40 is configured as the native VLAN for the 802.1Q trunk port from Customer X at the ingress edge switch in the service-provider network (Switch B). Switch A of Customer X sends a tagged packet on VLAN 30 to the ingress tunnel port of Switch B in the service-provider network, which belongs to access VLAN 40. Because the access VLAN of the tunnel port (VLAN 40) is the same as the native VLAN of the edge-switch trunk port (VLAN 40), the metro tag is not added to tagged packets received from the tunnel port. The packet carries only the VLAN 30 tag through the service-provider network to the trunk port of the egress-edge switch (Switch C) and is misdirected through the egress switch tunnel port to Customer Y.

These are some ways to solve this problem:

- Use ISL trunks between core switches in the service-provider network. Although customer interfaces connected to edge switches must be 802.1Q trunks, we recommend using ISL trunks for connecting switches in the core layer. The switch does not support ISL trunks.
- Use the **vlan dot1q tag native** global configuration command to configure the edge switch so that all packets going out an 802.1Q trunk, including the native VLAN, are tagged. If the switch is configured to tag native VLAN packets on all 802.1Q trunks, the switch accepts untagged packets, but sends only tagged packets.

- Ensure that the native VLAN ID on the edge-switch trunk port is not within the customer VLAN range. For example, if the trunk port carries traffic of VLANs 100 to 200, assign the native VLAN a number outside that range.

Figure 8-3 Potential Problem with 802.1Q Tunneling and Native VLANs



System MTU

The default system MTU for traffic on the switch is 1500 bytes. You can configure Fast Ethernet ports to support frames larger than 1500 bytes by using the **system mtu** global configuration command. You can configure Gigabit Ethernet ports to support frames larger than 1500 bytes by using the **system mtu jumbo** global configuration command. Because the 802.1Q tunneling feature increases the frame size by 4 bytes when the metro tag is added, you must configure all switches in the service-provider network to be able to process maximum frames by increasing the switch system MTU size to at least 1504 bytes. The maximum allowable system MTU for Gigabit Ethernet interfaces is 9000 bytes; the maximum system MTU for Fast Ethernet interfaces is 1998 bytes.

802.1Q Tunneling and Other Features

Although 802.1Q tunneling works well for Layer 2 packet switching, there are incompatibilities between some Layer 2 features and Layer 3 switching.

Note Layer 3 switching is supported only when the IP services image is running on the switch.

- A tunnel port cannot be a routed port.
- IP routing is not supported on a VLAN that includes 802.1Q tunnel ports. Packets received from a tunnel port are forwarded based only on Layer 2 information. If routing is enabled on a switch virtual interface (SVI) that includes tunnel ports, untagged IP packets received from the tunnel port are recognized and routed by the switch. Customers can access the internet through its native VLAN. If this access is not needed, you should not configure SVIs on VLANs that include tunnel ports.
- Tunnel ports do not support IP access control lists (ACLs).
- Layer 3 quality of service (QoS) ACLs and other QoS features related to Layer 3 information are not supported on tunnel ports. MAC-based QoS is supported on tunnel ports.
- EtherChannel port groups are compatible with tunnel ports as long as the 802.1Q configuration is consistent within an EtherChannel port group.
- UniDirectional Link Detection (UDLD) is supported on 802.1Q tunnel ports.
- Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP) are supported only on 802.1Q tunnel ports that are network node interfaces (NNIs) or enhanced network interfaces (ENIs). UNIs do not support PAgP and LACP.
- Loopback detection is supported on 802.1Q tunnel ports.
- When an NNI or ENI port is configured as an 802.1Q tunnel port, spanning-tree bridge protocol data unit (BPDU) filtering is automatically enabled on the interface, and the Cisco Discovery Protocol (CDP) and the Layer Link Discovery Protocol (LLDP) are automatically disabled on the interface. UNIs do not support BPDU filtering, CDP, or LLDP.
- In a UNI-ENI isolated VLAN, 802.1Q tunneled access ports are isolated from each other, but in a UNI-ENI community VLAN, local switching occurs between these ports. For more information about UNI-ENI VLANs, see Chapter 3, “Configuring VLANs.”

Default Settings

By default, 802.1Q tunneling is disabled because the default switchport mode is access. Tagging of 802.1Q native VLAN packets on all 802.1Q trunk ports is also disabled. By default, VLANs on the switch are UNI-ENI isolated VLANs.

Configuring an 802.1Q Tunneling Port

BEFORE YOU BEGIN

Review the “Guidelines and Limitations” section on page 8-4.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode for the interface to be configured as a tunnel port. This should be the edge port in the service-provider network that connects to the customer switch. Valid interfaces include physical interfaces and port-channel logical interfaces (port channels 1 to 48).
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	**switchport access vlan** *vlan-id*	Specify the default VLAN, which is used if the interface stops trunking. This VLAN ID is specific to the particular customer. **Note** If the VLAN is a UNI-ENI isolated VLAN, local switching does not occur between UNIs and ENIs on the switch. If the VLAN is a UNI-ENI community VLAN, local switching is allowed.
Step 5	**switchport mode dot1q-tunnel**	Set the interface as an 802.1Q tunnel port.
Step 6	**exit**	Return to global configuration mode.
Step 7	**vlan dot1q tag native**	(Optional) Set the switch to enable tagging of native VLAN packets on all 802.1Q trunk ports. When not set, and a customer VLAN ID is the same as the native VLAN, the trunk port does not apply a metro tag, and packets could be sent to the wrong destination.
Step 8	**end**	Return to privileged EXEC mode.
Step 9	**show running-config**	Display the ports configured for 802.1Q tunneling.
	show dot1q-tunnel	Display the ports that are in tunnel mode.
Step 10	**show vlan dot1q tag native**	Display 802.1Q native VLAN tagging status.
Step 11	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no switchport mode dot1q-tunnel** interface configuration command to return the port to the default state of access. Use the **no vlan dot1q tag native** global configuration command to disable tagging of native VLAN packets.

EXAMPLE

This example shows how to configure an interface as a tunnel port, enable tagging of native VLAN packets, and verify the configuration. In this configuration, the VLAN ID for the customer connected to Gigabit Ethernet interface 2 is VLAN 22. This VLAN is by default a UNI-ENI isolated VLAN.

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport access vlan 22
% Access VLAN does not exist. Creating vlan 22
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# exit
Switch(config)# vlan dot1q tag native
Switch(config)# end
```

```
Switch# show dot1q-tunnel interface gigabitethernet0/2
dot1q-tunnel mode LAN Port(s)
-----------------------------
Gi0/1

Switch# show vlan dot1q tag native
dot1q native vlan tagging is enabled
```

Verifying Configuration

Command	Purpose
show dot1q-tunnel	Display 802.1Q tunnel ports on the switch.
show dot1q-tunnel interface *interface-id*	Verify if a specific interface is a tunnel port.
show vlan dot1q tag native	Display the status of native VLAN tagging on the switch.

Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS LAN Switching Command Reference
- Cisco IOS Interface and Hardware Component Command Reference

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520 Switch	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

Configuring VLAN Mapping

The Cisco 2520 Connected Grid Switch (CGS 2520) supports VLAN mapping (or VLAN ID translation) on trunk ports.

Note VLAN Mapping is not supported on the Cisco Industrial Ethernet 2000U Series (IE 2000U) switch or the Ethernet Switch Module (ESM) for CGR 2010.

This chapter includes the following sections:

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 9-8.

Information About VLAN Mapping

Another way to establish service provider VLANs is to configure VLAN mapping (or VLAN ID translation) on trunk ports connected to a customer network to map customer VLANs to service-provider VLANs. Packets entering the port are mapped to a service provider VLAN (S-VLAN) based on the port number and the original customer VLAN-ID (C-VLAN) of the packet.

In a typical metro deployment, VLAN mapping takes place on user network interfaces (UNIs) or enhanced network interfaces (ENIs) that face the customer network. However, you are not prevented from configuring VLAN mapping on network node interfaces (NNIs).

Because the VLAN ID is mapped to the S-VLAN on ingress, on the switch all forwarding operations are performed by using S-VLAN information and not C-VLAN information.

Note When you configure features on a port that has VLAN mapping configured, you always use the S-VLAN (translated VLAN) ID, not the customer VLAN-ID (C-VLAN).

On an interface configured for VLAN mapping, the specified C-VLAN packets are mapped to the specified S-VLAN when they enter the port. Symmetrical mapping back to the customer C-VLAN occurs when packets exit the port.

The switch supports these types of VLAN mapping on UNI trunk ports:

- One-to-one VLAN mapping occurs at the ingress and egress of the port and maps the customer C-VLAN ID in the 802.1Q tag to the service-provider S-VLAN ID. You can also specify that packets with all other VLAN IDs are dropped.
- Selective QinQ maps the specified customer VLANs entering the UNI to the specified S-VLAN ID. The S-VLAN is added to the incoming unmodified C-VLAN. You can also specify that traffic carrying all other customer VLAN IDs is dropped.
- Traditional 802.1Q tunneling (QinQ) performs all-to-one bundling of C-VLAN IDs to a single S-VLAN ID for the port. The S-VLAN is added to the incoming unmodified C-VLAN. You can configure the UNI as an 802.1Q tunnel port for traditional QinQ, or you can configure selective QinQ on trunk ports for a more flexible implementation. Mapping takes place at ingress and egress of the port. All packets on the port are bundled into the specified S-VLAN.

Note Untagged packets enter the switch on the trunk native VLAN and are not mapped.

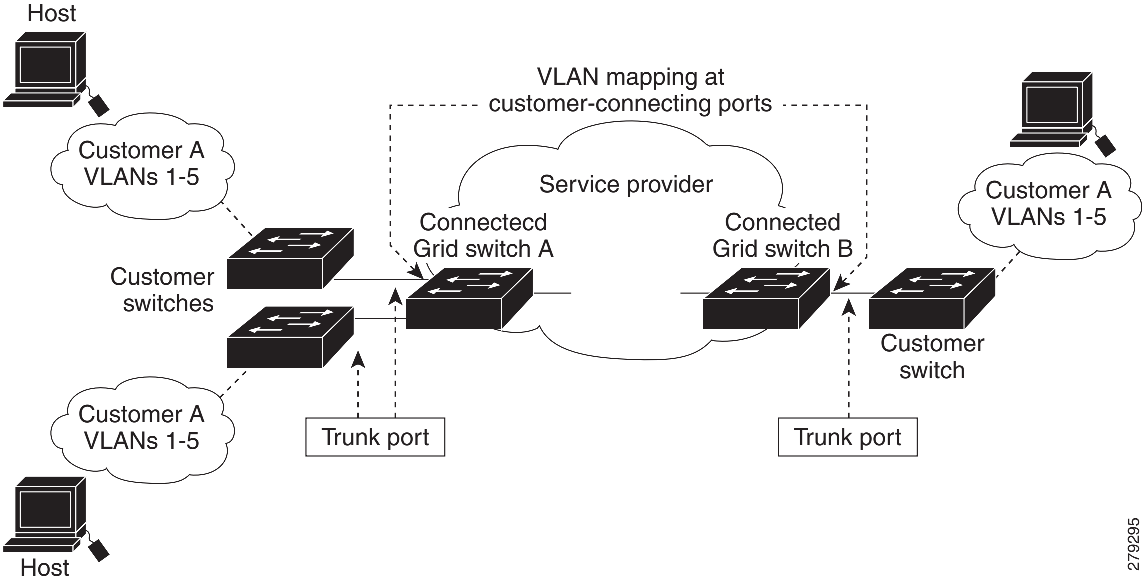
For quality of service (QoS), the switch has flexible mapping between C-CoS or C-DSCP and S-CoS and maps the inner CoS to the outer CoS for traffic with traditional QinQ or selective QinQ VLAN mapping. For more information, see the “802.1Q Tunneling CoS Mapping” section in the *QoS Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.

Mapping Customer VLANs to Service-Provider VLANs

Figure 9-1 shows a topology where a customer uses the same VLANs in multiple sites on different sides of a service-provider network. You map the customer VLAN IDs to service-provider VLAN IDs for packet travel across the service-provider backbone. The customer VLAN IDs are retrieved at the other side of the service-provider backbone for use in the other customer site. Configure the same set of VLAN mappings at a customer-connected port on each side of the service-provider network.

See the examples following the configuration steps for using one-to-one mapping, traditional QinQ, or selective QinQ to map customer VLANs 1 to 5 to service-provider VLANs.

Figure 9-1 Mapping Customer VLANs



Prerequisites

- Be familiar with the information in the "Information About VLAN Mapping" section on page 9-1 and "Guidelines and Limitations" section on page 9-3.
- Ensure that your network strategy and planning for your network are complete. For example, you must decide what type of VLAN mapping your network requires.

Guidelines and Limitations

- Traditional QinQ uses 802.1Q tunnel ports; you configure one-to-one VLAN mapping and selective QinQ on 802.1Q trunk ports.
- To avoid mixing customer traffic, when you configure traditional Q-in-Q on a trunk port, you should configure the service provider S-VLAN ID as an allowed VLAN on the trunk port.
- On a switch interface configured for VLAN mapping, mapping to the S-VLAN occurs on traffic entering the switch. Therefore, when you configure other features on an interface configured for VLAN mapping, you should use the S-VLAN ID, except when configuring VLAN mapping and Ethernet E-LMI. When configuring E-LMI on an interface, use the C-VLAN when entering the **ethernet lmi ce-vlan map** *vlan-id* service instance configuration mode command.
- When you configure VLAN mapping on an EtherChannel, the mapping applies to all ports in the port channel.
- You cannot configure encapsulation replicate on a SPAN destination port if the source port is configured as a tunnel port or has a 1-to-2 mapping configured. Encapsulation replicate is supported with 1-to-1 VLAN mapping.
- To determine switch resources used for VLAN mapping, enter the **show vlan mapping usage** or **show platform vlan mapping** privileged EXEC command.

Default Settings

By default, no VLAN mapping is configured.

Configuring VLAN Mapping

These procedures show how to configure each type of VLAN mapping on trunk ports. To verify your configuration, enter the **show interfaces** *interface-id* **vlan mapping** or **show vlan mapping** privileged EXEC commands. See the "Verifying Configuration" section on page 9-7 for the syntax of these commands.

One-to-One Mapping

Follow this procedure to configure one-to-one VLAN mapping to map a customer VLAN ID to a service-provider VLAN ID. You can use the **default drop** keywords to specify that traffic is dropped unless both the specified C-VLAN ID and S-VLAN ID combination is explicitly mapped.

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 9-3.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode for the interface connected to the service-provider network. You can enter a physical interface or an EtherChannel port channel.
Step 3	**switchport mode trunk**	Configure the interface as a trunk port.
Step 4	**switchport vlan mapping** *vlan-id translated-id*	Enter the VLAN IDs to be mapped: • *vlan-id*—the customer VLAN ID (C-VLAN) entering the switch from the customer network. The range is from 1 to 4094. • *translated-id*—the assigned service-provider VLAN ID (S-VLAN). The range is from 1 to 4094.
Step 5	**switchport vlan mapping default drop**	(Optional) Specify that all packets on the port are dropped if they do not match the VLANs specified in Step 4.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show vlan mapping**	Verify the configuration.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no switchport vlan mapping** *vlan-id translated-id* command to remove the VLAN mapping information. Entering **no switchport vlan mapping all** deletes all mapping configurations.

EXAMPLE

This example shows how to map VLAN IDs 1 to 5 in the customer network to VLANs 101 to 105 in the service-provider network as shown in Figure 9-1. You configure these same VLAN mapping commands for a port in Switch A and Switch B. The traffic on any other VLAN IDs is dropped.

```
Switch(config)# interface gigabiethernet0/1
Switch(config-if)# switchport vlan mapping 1 101
Switch(config-if)# switchport vlan mapping 2 102
Switch(config-if)# switchport vlan mapping 3 103
Switch(config-if)# switchport vlan mapping 4 104
Switch(config-if)# switchport vlan mapping 4 105
Switch(config-if)# switchport vlan mapping default drop
Switch(config-if)# exit
```

In the previous example, at the ingress of the service-provider network, VLAN IDs 1 to 5 in the customer network are mapped to VLANs 101 to 105, respectively, inside of the service-provider network. At the egress of the service-provider network, VLANs 101 to 105 in the service-provider network are mapped to VLAN IDs 1 to 5, respectively, in the customer network.

Traditional QinQ on a Trunk Port

Follow this procedure to configure VLAN mapping for traditional QinQ on a trunk port or tunneling by default. Configuring tunneling by default bundles all packets on the port into the configured S-VLAN.

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 9-3.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode for the interface connected to the service-provider network. You can enter a physical interface or an EtherChannel port channel.
Step 3	**switchport mode trunk**	Configure the interface as a trunk port.
Step 4	switchport trunk allowed vlan *vlan-id*	Configure the outer VLAN of the service provider network (S-VLAN) to to be allowed on the interface. This should be the same outer VLAN ID entered in the next step.
Step 5	**switchport vlan mapping default dot1q-tunnel** *outer vlan-id*	Configure VLAN mapping so that all packets entering the port are bundled into the specified S-VLAN: *outer-vlan-id*—Enter the outer VLAN ID (S-VLAN) of the service-provider network. The range is from 1 to 4094.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show interfaces** *interface-id* **vlan mapping**	Verify the configuration.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no switchport vlan mapping tunnel default** *outer vlan-id* command to remove the VLAN mapping configuration. Entering **no switchport vlan mapping all** deletes all mapping configurations.

EXAMPLE

This example shows how to bundle all traffic on the port to leave the switch with the S-VLAN ID of 100:

```
Switch(config)# interface gigabiethernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed 100
Switch(config-if)# switchport vlan mapping default dot1q-tunnel 100
Switch(config-if)# exit
```

Selective QinQ on a Trunk Port

Follow this procedure to configure VLAN mapping for selective QinQ on a trunk port. Note that you can configure one-to-one mapping and selective QinQ on the same interface, but you cannot use the same C-VLAN IDs in both configurations. You can use the **default drop** keywords to specify that traffic is dropped unless the specified C-VLAN ID and S-VLAN ID combination is explicitly mapped.

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 9-3.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode for the interface connected to the service-provider network. You can enter a physical interface or an EtherChannel port channel.
Step 3	**switchport mode trunk**	Configure the interface as a trunk port.
Step 4	**switchport vlan mapping** *vlan-id* **dot1q-tunnel** *outer vlan-id*	Enter the VLAN IDs to be mapped: • *vlan-id*—the customer VLAN ID (C-VLAN) entering the switch from the customer network. The range is from 1 to 4094. You can enter a string of VLAN-IDs. • *outer-vlan-id*—Enter the outer VLAN ID (S-VLAN) of the service-provider network. The range is from 1 to 4094.
Step 5	**switchport vlan mapping default drop**	(Optional) Specify that all packets on the port are dropped if they do not match the VLANs specified in Step 4.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show interfaces** *interface-id* **vlan mapping**	Verify the configuration.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no switchport vlan mapping** *vlan-id* **dot1q-tunnel** *outer vlan-id* command to remove the VLAN mapping configuration. Entering **no switchport vlan mapping all** deletes all mapping configurations.

EXAMPLE

This example shows how to configure selective QinQ mapping on the port so that traffic with a C-VLAN ID of 1 to 5 enters the switch with an S-VLAN ID of 100. The traffic of any other VLAN IDs is dropped.

```
Switch(config)# interface gigabiethernet0/1
Switch(config-if)# switchport vlan mapping 1-5 dot1q-tunnel 100
Switch(config-if)# switchport vlan mapping default drop
Switch(config-if)# exit
```

Verifying Configuration

Command	Purpose
show interfaces [**interface** *interface-id*] **vlan mapping**	Display VLAN mapping information for all interfaces or for the specified interface.
show platform vlan mapping	Display platform VLAN mapping information.
show vlan mapping [*interface-id*]	Display VLAN mapping information for all interfaces or for the specified interface.
show vlan mapping usage	Display information about hardware resource usage on the switch devoted to VLAN mapping.

Configuration Example

This example shows how to map VLAN IDs 1 to 5 in the customer network to VLANs 101 to 105 in the service-provider network as shown in Figure 9-1. You configure these same VLAN mapping commands for a port in Switch A and Switch B. The traffic on any other VLAN IDs is dropped.

```
Switch(config)# interface gigabiethernet0/1
Switch(config-if)# switchport vlan mapping 1 101
Switch(config-if)# switchport vlan mapping 2 102
Switch(config-if)# switchport vlan mapping 3 103
Switch(config-if)# switchport vlan mapping 4 104
Switch(config-if)# switchport vlan mapping 4 105
Switch(config-if)# switchport vlan mapping default drop
Switch(config-if)# exit
```

This example shows how to bundle all traffic on the port to leave the switch with the S-VLAN ID of 100:

```
Switch(config)# interface gigabiethernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed 100
Switch(config-if)# switchport vlan mapping default dot1q-tunnel 100
Switch(config-if)# exit
```

This example shows how to configure selective QinQ mapping on the port so that traffic with a C-VLAN ID of 1 to 5 enters the switch with an S-VLAN ID of 100. The traffic of any other VLAN IDs is dropped.

```
Switch(config)# interface gigabiethernet0/1
Switch(config-if)# switchport vlan mapping 1-5 dot1q-tunnel 100
Switch(config-if)# switchport vlan mapping default drop
Switch(config-if)# exit
```

Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS LAN Switching Command Reference
- Cisco IOS Interface and Hardware Component Command Reference
- QoS Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches

Feature History

Platform	First Supported Release
CGS 2520 Switch	Cisco IOS Release 12.2(53)EX

CHAPTER 10

Configuring Layer 2 Protocol Tunneling

This chapter describes how to configure Layer 2 protocol tunneling on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*.

Virtual private networks (VPNs) provide enterprise-scale connectivity on a shared infrastructure, often Ethernet-based, with the same security, prioritization, reliability, and manageability requirements of private networks. Tunneling is a feature designed for service providers who carry traffic of multiple customers across their networks and are required to maintain the VLAN and Layer 2 protocol configurations of each customer without impacting the traffic of other customers. The switch supports IEEE 802.1Q tunneling and Layer 2 protocol tunneling; IEEE 802.1Q tunneling is described in Chapter 8, “Configuring IEEE 802.1Q Tunneling.”

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the “Related Documents” section on page 10-14.

This chapter includes the following sections:

Information About Layer 2 Protocol Tunneling

Customers at different sites connected across a service-provider network need to use various Layer 2 protocols to scale their topologies to include all remote sites, as well as the local sites. STP must run properly, and every VLAN should build a proper spanning tree that includes the local site and all remote sites across the service-provider network. Cisco Discovery Protocol (CDP) must discover neighboring Cisco devices from local and remote sites. VLAN Trunking Protocol (VTP) must provide consistent VLAN configuration throughout all sites in the customer network that are participating in VTP.

Note CDP and STP are supported by default on NNIs and can be enabled on ENIs. However, Layer 2 protocol tunneling is supported on all ports on the switch.

When protocol tunneling is enabled, edge switches on the inbound side of the service-provider network encapsulate Layer 2 protocol packets with a special MAC address and send them across the service-provider network. Core switches in the network do not process these packets but forward them as normal packets. Layer 2 protocol data units (PDUs) for CDP, STP, or VTP cross the service-provider network and are delivered to customer switches on the outbound side of the service-provider network. Identical packets are received by all customer ports on the same VLANs with these results:

- Users on each of a customer's sites can properly run STP, and every VLAN can build a correct spanning tree based on parameters from all sites and not just from the local site.
- CDP discovers and shows information about the other Cisco devices connected through the service-provider network.
- VTP provides consistent VLAN configuration throughout the customer network, propagating to all switches through the service provider that support VTP.

Note To provide interoperability with third-party vendors, you can use the Layer 2 protocol-tunnel bypass feature. Bypass mode transparently forwards control PDUs to vendor switches that have different ways of controlling protocol tunneling. You implement bypass mode by enabling Layer 2 protocol tunneling on the egress trunk port. When Layer 2 protocol tunneling is enabled on the trunk port, the encapsulated tunnel MAC address is removed and the protocol packets have their normal MAC address.

Layer 2 protocol tunneling can be used independently or can enhance 802.1Q tunneling. If protocol tunneling is not enabled on 802.1Q tunneling ports, remote switches at the receiving end of the service-provider network do not receive the PDUs and cannot properly run STP, CDP, and VTP. When protocol tunneling *is* enabled, Layer 2 protocols within each customer's network are totally separate from those running within the service-provider network. Customer switches on different sites that send traffic through the service-provider network with 802.1Q tunneling achieve complete knowledge of the customer's VLAN. If 802.1Q tunneling is not used, you can still enable Layer 2 protocol tunneling by connecting to the customer switch through access or trunk ports and enabling tunneling on the service-provider access or trunk port.

For example, in Figure 10-1, Customer X has four switches in the same VLAN, that are connected through the service-provider network. If the network does not tunnel PDUs, switches on the far ends of the network cannot properly run STP, CDP, and VTP. For example, STP for a VLAN on a switch in Customer X, Site 1, will build a spanning tree on the switches at that site without considering convergence parameters based on Customer X's switch in Site 2. This could result in the topology shown in Figure 10-2.

Figure 10-1 Layer 2 Protocol Tunneling

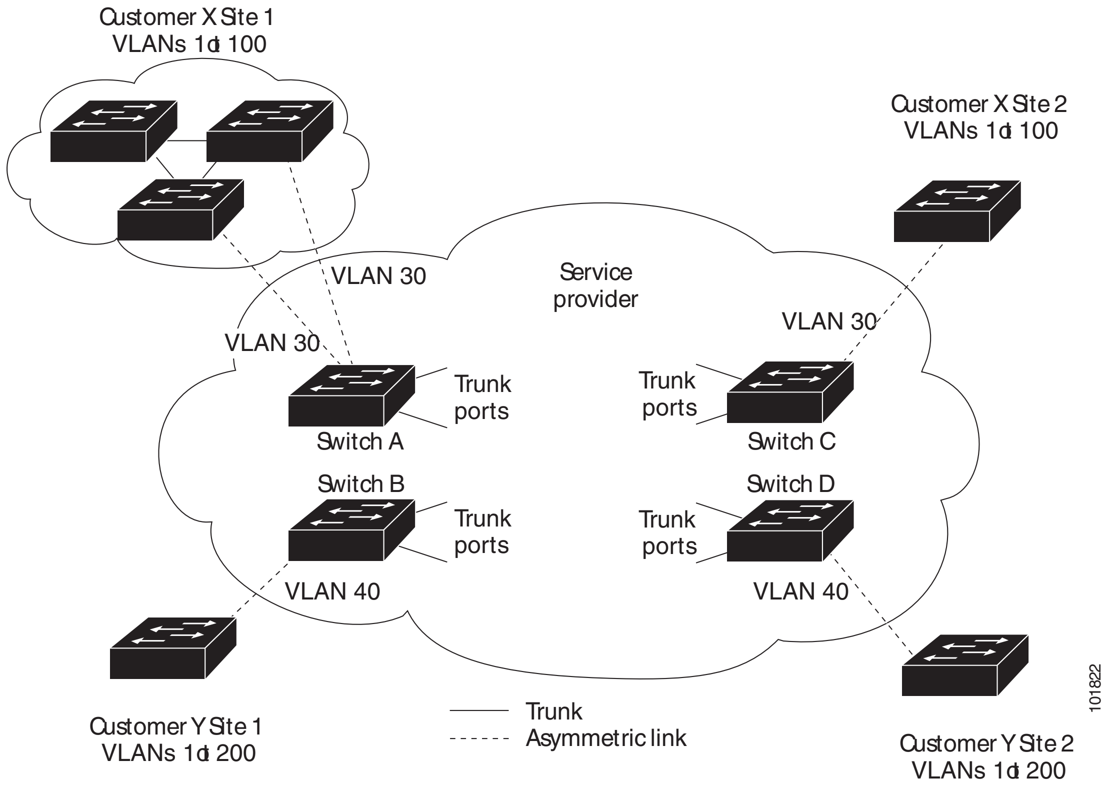
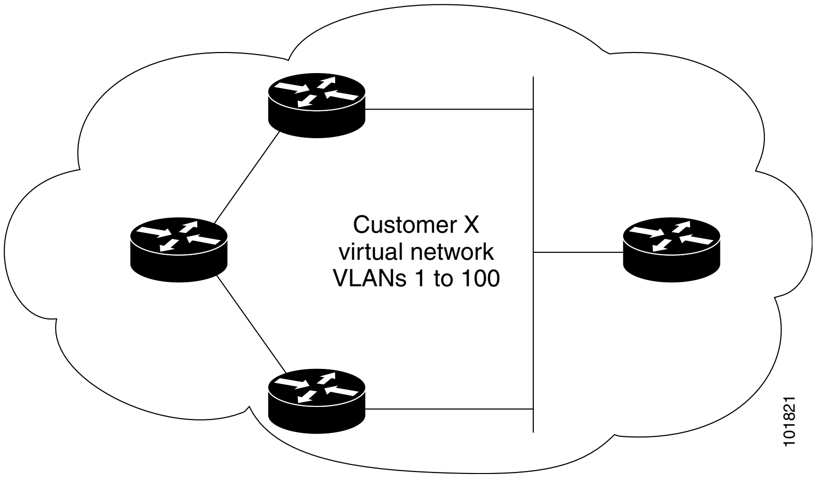


Figure 10-2 Layer 2 Network Topology without Proper Convergence

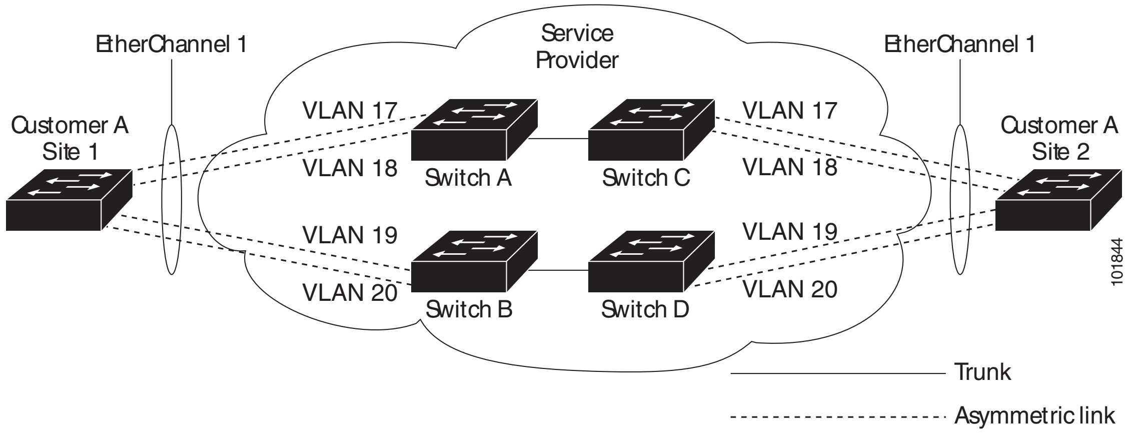


In an SP network, you can use Layer 2 protocol tunneling to enhance the creation of EtherChannels by emulating a point-to-point network topology. When you enable protocol tunneling (PAgP or LACP) on the SP switch, remote customer switches receive the PDUs and can negotiate the automatic creation of EtherChannels.

For example, in Figure 10-3, Customer A has two switches in the same VLAN that are connected through the SP network. When the network tunnels PDUs, switches on the far ends of the network can negotiate the automatic creation of EtherChannels without needing dedicated lines. See the "Configuring

Layer 2 Tunneling for EtherChannels" section on page 10-8 for instructions.

Figure 10-3 Layer 2 Protocol Tunneling for EtherChannels



Prerequisites

- Be familiar with the information in the "Information About Layer 2 Protocol Tunneling" section on page 10-1 and "Guidelines and Limitations" section on page 10-4.
- Ensure that your network strategy and planning for your network are complete.

Guidelines and Limitations

These are some configuration guidelines and operating characteristics of Layer 2 protocol tunneling:

- The switch supports tunneling of CDP, STP, including multiple STP (MSTP), and VTP. Protocol tunneling is disabled by default but can be enabled for the individual protocols on 802.1Q tunnel ports, access ports. or trunk ports.
- The edge switches on the outbound side of the service-provider network restore the proper Layer 2 protocol and MAC address information and forward the packets to all Layer 2 protocol-enabled tunnel, access, and trunk ports in the same metro VLAN.
- For interoperability with third-party vendor switches, the switch supports a Layer 2 protocol-tunnel bypass feature. Bypass mode transparently forwards control PDUs to vendor switches that have different ways of controlling protocol tunneling.When Layer 2 protocol tunneling is enabled on ingress ports on a switch, egress trunk ports forward the tunneled packets with a special encapsulation. If you also enable Layer 2 protocol tunneling on the egress trunk port, this behavior is bypassed, and the switch forwards control PDUs without any processing or modification.
- The switch supports PAgP, LACP, and UDLD tunneling for emulated point-to-point network topologies. Protocol tunneling is disabled by default but can be enabled for the individual protocols on 802.1Q tunnel ports, access ports, or trunk ports.
- If you enable PAgP or LACP tunneling, we recommend that you also enable UDLD on the interface for faster link-failure detection.
- Loopback detection is not supported on Layer 2 protocol tunneling of PAgP, LACP, or UDLD packets.

- EtherChannel port groups are compatible with tunnel ports when the 802.1Q configuration is consistent within an EtherChannel port group.
- If an encapsulated PDU (with the proprietary destination MAC address) is received from a tunnel port or access or trunk port with Layer 2 tunneling enabled, the tunnel port is shut down to prevent loops. The port also shuts down when a configured shutdown threshold for the protocol is reached. You can manually re-enable the port (by entering a **shutdown** and a **no shutdown** command sequence). If errdisable recovery is enabled, the operation is retried after a specified time interval.
- Only decapsulated PDUs are forwarded to the customer network. The spanning-tree instance running on the service-provider network does not forward BPDUs to tunnel ports. CDP packets are not forwarded from tunnel ports.
- When protocol tunneling is enabled on an interface, you can set a per-protocol, per-port, shutdown threshold for the PDUs generated by the customer network. If the limit is exceeded, the port shuts down. You can also limit BPDU rate by using QoS ACLs and policy maps on a tunnel port.
- When protocol tunneling is enabled on an interface, you can set a per-protocol, per-port, drop threshold for the PDUs generated by the customer network. If the limit is exceeded, the port drops PDUs until the rate at which it receives them is below the drop threshold.
- Because tunneled PDUs (especially STP BPDUs) must be delivered to all remote sites so that the customer virtual network operates properly, you can give PDUs higher priority within the service-provider network than data packets received from the same tunnel port. By default, the PDUs use the same CoS value as data packets.

Default Settings

Feature	Default Setting
Layer 2 protocol tunneling	Disabled.
Shutdown threshold	None set.
Drop threshold	None set.
CoS value	If a CoS value is configured on the interface, that value is used to set the BPDU CoS value for Layer 2 protocol tunneling. If no CoS value is configured at the interface level, the default value for CoS marking of L2 protocol tunneling BPDUs is 5. This does not apply to data traffic.

Configuring Layer 2 Protocol Tunneling

You can enable Layer 2 protocol tunneling (by protocol) on the ports that are connected to the customer in the edge switches of the service-provider network. The service-provider edge switches connected to the customer switch perform the tunneling process. Edge-switch tunnel ports are connected to customer 802.1Q trunk ports. Edge-switch access ports are connected to customer access ports. The edge switches connected to the customer switch perform the tunneling process.

You can enable Layer 2 protocol tunneling on ports that are configured as access ports, tunnel ports, or trunk ports. The switch supports Layer 2 protocol tunneling for CDP, STP, and VTP. For emulated point-to-point network topologies, it also supports PAgP, LACP, and UDLD protocols. The switch does not support Layer 2 protocol tunneling for LLDP.

Caution PAgP, LACP, and UDLD protocol tunneling is only intended to emulate a point-to-point topology. An erroneous configuration that sends tunneled packets to many ports could lead to a network failure.

When the Layer 2 PDUs that entered the service-provider inbound edge switch through a Layer 2 protocol-enabled port exit through the trunk port into the service-provider network, the switch overwrites the customer PDU-destination MAC address with a well-known Cisco proprietary multicast address (01-00-0c-cd-cd-d0). If 802.1Q tunneling is enabled, packets are also double-tagged; the outer tag is the customer metro tag, and the inner tag is the customer's VLAN tag. The core switches ignore the inner tags and forward the packet to all trunk ports in the same metro VLAN. The edge switches on the outbound side restore the proper Layer 2 protocol and MAC address information and forward the packets to all Layer 2 protocol-enabled access ports, tunnel ports, and trunk ports in the same metro VLAN. Therefore, the Layer 2 PDUs remain intact and are delivered across the service-provider infrastructure to the other side of the customer network.

See Figure 10-1, with Customer X and Customer Y in access VLANs 30 and 40, respectively. Asymmetric links connect the customers in Site 1 to edge switches in the service-provider network. The Layer 2 PDUs (for example, BPDUs) coming into Switch B from Customer Y in Site 1 are forwarded to the infrastructure as double-tagged packets with the well-known MAC address as the destination MAC address. These double-tagged packets have the metro VLAN tag of 40, as well as an inner VLAN tag (for example, VLAN 100). When the double-tagged packets enter Switch D, the outer VLAN tag 40 is removed, the well-known MAC address is replaced with the respective Layer 2 protocol MAC address, and the packet is sent to Customer Y on Site 2 as a single-tagged frame in VLAN 100.

You can also enable Layer 2 protocol tunneling on access ports on the edge switch connected to access or trunk ports on the customer switch. In this case, the encapsulation and decapsulation process is the same as described in the previous paragraph, except that the packets are not double-tagged in the service-provider network. The single tag is the customer-specific access VLAN tag.

This section includes the following topics:

- Configuring a Port for Layer 2 Protocol Tunneling, page 10-6
- Configuring Layer 2 Tunneling for EtherChannels, page 10-8

Configuring a Port for Layer 2 Protocol Tunneling

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 10-4.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and enter the interface to be configured as a tunnel port. This should be the edge port in the service-provider network that connects to the customer switch. Valid interfaces can be physical interfaces and port-channel logical interfaces (port channels 1 to 48).

	Command	Purpose
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	**switchport mode access** or **switchport mode dot1q-tunnel** or **switchport mode trunk**	Configure the interface as an access port, an 802.1Q tunnel port or a trunk port. The default switchport mode is access.
Step 5	**l2protocol-tunnel** [**cdp** | **stp** | **vtp**]	Enable protocol tunneling for the desired protocol. If no keyword is entered, tunneling is enabled for all three Layer 2 protocols.
Step 6	**l2protocol-tunnel shutdown-threshold** [**cdp** | **stp** | **vtp**] *value*	(Optional) Configure the threshold for packets-per-second accepted for encapsulation. The interface is disabled if the configured threshold is exceeded. If no protocol option is specified, the threshold applies to each of the tunneled Layer 2 protocol types. The range is 1 to 4096. The default is to have no threshold configured. **Note** If you also set a drop threshold on this interface, the shutdown-threshold value must be greater than or equal to the drop-threshold value.
Step 7	**l2protocol-tunnel drop-threshold** [**cdp** | **stp** | **vtp**] *value*	(Optional) Configure the threshold for packets-per-second accepted for encapsulation. The interface drops packets if the configured threshold is exceeded. If no protocol option is specified, the threshold applies to each of the tunneled Layer 2 protocol types. The range is 1 to 4096. The default is to have no threshold configured. If you also set a shutdown threshold on this interface, the drop-threshold value must be less than or equal to the shutdown-threshold value.
Step 8	**exit**	Return to global configuration mode.
Step 9	**errdisable recovery cause l2ptguard**	(Optional) Configure the recovery mechanism from a Layer 2 maximum-rate error so that the interface is re-enabled and can try again. Errdisable recovery is disabled by default; when enabled, the default time interval is 300 seconds.
Step 10	**l2protocol-tunnel cos** *value*	(Optional) Configure the CoS value for all tunneled Layer 2 PDUs. The range is 0 to 7; the default is the default CoS value for the interface. If none is configured, the default is 5.
Step 11	**end**	Return to privileged EXEC mode.
Step 12	**show l2protocol**	Display the Layer 2 tunnel ports on the switch, including the protocols configured, the thresholds, and the counters.
Step 13	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no l2protocol-tunnel** [**cdp** | **stp** | **vtp**] interface configuration command to disable protocol tunneling for one of the Layer 2 protocols or for all three. Use the **no l2protocol-tunnel shutdown-threshold** [**cdp** | **stp** | **vtp**] and the **no l2protocol-tunnel drop-threshold** [**cdp** | **stp** | **vtp**] commands to return the shutdown and drop thresholds to the default settings.

EXAMPLE

This example shows how to configure Layer 2 protocol tunneling for CDP, STP, and VTP and to verify the configuration.

```
Switch(config)# interface gigaethernet0/1
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# l2protocol-tunnel stp
Switch(config-if)# l2protocol-tunnel vtp
Switch(config-if)# l2protocol-tunnel shutdown-threshold 1500
Switch(config-if)# l2protocol-tunnel drop-threshold 1000
Switch(config-if)# exit
Switch(config)# l2protocol-tunnel cos 7
Switch(config)# end
Switch# show l2protocol
COS for Encapsulated Packets: 7
Port      Protocol Shutdown  Drop      Encapsulation Decapsulation Drop
                   Threshold Threshold Counter       Counter       Counter
-------   -------- --------- --------- ------------- ------------- -------------
Gi  0/1  cdp           1500      1000 2288          2282          0
          stp           1500      1000 116           13            0
          vtp           1500      1000 3             67            0
          pagp          ----      ---- 0             0             0
          lacp          ----      ---- 0             0             0
          udld          ----      ---- 0             0             0
```

Configuring Layer 2 Tunneling for EtherChannels

To configure Layer 2 point-to-point tunneling to facilitate the creation of EtherChannels, you need to configure both the SP edge switch and the customer switch. (See Figure 10-3 on page 10-4.)

Configuring the SP Edge Switch

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 10-4.

Caution To avoid a network failure, make sure that the network is a point-to-point topology before you enable tunneling for PAgP, LACP, or UDLD packets.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and enter the interface to be configured as a tunnel port. This should be the edge port in the SP network that connects to the customer switch. Valid interfaces are physical interfaces.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	**switchport mode dot1q-tunnel**	Configure the interface as an 802.1Q tunnel port.

	Command	Purpose
Step 5	**l2protocol-tunnel point-to-point** [**pagp** | **lacp** | **udld**]	(Optional) Enable point-to-point protocol tunneling for the desired protocol. If no keyword is entered, tunneling is enabled for all three protocols.
Step 6	**l2protocol-tunnel shutdown-threshold** [**point-to-point** [**pagp** | **lacp** | **udld**]] *value*	(Optional) Configure the threshold for packets-per-second accepted for encapsulation. The interface is disabled if the configured threshold is exceeded. If no protocol option is specified, the threshold applies to each of the tunneled Layer 2 protocol types. The range is 1 to 4096. The default is to have no threshold configured. **Note** If you also set a drop threshold on this interface, the shutdown-threshold value must be greater than or equal to the drop-threshold value.
Step 7	**l2protocol-tunnel drop-threshold** [**point-to-point** [**pagp** | **lacp** | **udld**]] *value*	(Optional) Configure the threshold for packets-per-second accepted for encapsulation. The interface drops packets if the configured threshold is exceeded. If no protocol option is specified, the threshold applies to each of the tunneled Layer 2 protocol types. The range is 1 to 4096. The default is to have no threshold configured. **Note** If you also set a shutdown threshold on this interface, the drop-threshold value must be less than or equal to the shutdown-threshold value.
Step 8	**no cdp enable**	If the interface is an NNI, disable CDP on the interface. CDP is disabled by default on ENIs. UNIs do not support CDP.
Step 9	**spanning-tree bpdufilter enable**	If the interface is an NNI or ENI, enable BPDU filtering on the interface. UNIs do not support STP PBDU filtering.
Step 10	**exit**	Return to global configuration mode.
Step 11	**errdisable recovery cause l2ptguard**	(Optional) Configure the recovery mechanism from a Layer 2 maximum-rate error so that the interface is re-enabled and can try again. Errdisable recovery is disabled by default; when enabled, the default time interval is 300 seconds.
Step 12	**l2protocol-tunnel cos** *value*	(Optional) Configure the CoS value for all tunneled Layer 2 PDUs. The range is 0 to 7; the default is the default CoS value for the interface. If none is configured, the default is 5.
Step 13	**end**	Return to privileged EXEC mode.
Step 14	**show l2protocol**	Display the Layer 2 tunnel ports on the switch, including the protocols configured, the thresholds, and the counters.
Step 15	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no l2protocol-tunnel** [**point-to-point** [**pagp** | **lacp** | **udld**]] interface configuration command to disable point-to-point protocol tunneling for one of the Layer 2 protocols or for all three. Use the **no l2protocol-tunnel shutdown-threshold** [**point-to-point** [**pagp** | **lacp** | **udld**]] and the **no l2protocol-tunnel drop-threshold** [[**point-to-point** [**pagp** | **lacp** | **udld**]] commands to return the shutdown and drop thresholds to the default settings.

EXAMPLE

This example shows how to configure the SP edge switch 1 and edge switch 2. VLANs 17, 18, 19, and 20 are the access VLANs, Gigabit Ethernet interfaces 1 and 2 are point-to-point tunnel ports with PAgP and UDLD enabled, the drop threshold is 1000, and Fast Ethernet interface 3 is a trunk port.

SP edge switch 1 configuration:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport access vlan 17
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport access vlan 18
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet0/3
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
```

SP edge switch 2 configuration:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport access vlan 19
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport access vlan 20
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet0/3
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
```

Configuring the Customer Switch

For EtherChannels, you need to configure both the SP edge switches and the customer switches for Layer 2 protocol tunneling. (See Figure 10-3 on page 10-4.)

BEFORE YOU BEGIN

Configure the SP edge switch as described in the "Configuring the SP Edge Switch" procedure on page 10-8.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter the interface configuration mode. This should be the customer switch port.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled and NNIs are enabled.
Step 4	**switchport mode trunk**	Enable trunking on the interface.
Step 5	**udld enable**	Enable UDLD in **normal** mode on the interface.
Step 6	**channel-group** *channel-group-number* **mode desirable**	Assign the interface to a channel group, and specify **desirable** for the PAgP mode if the interface is an NNI or ENI. For more information about configuring EtherChannels, see the "Configuring EtherChannels and Link State Tracking" chapter in the *High Availability and Redundancy Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.
Step 7	**exit**	Return to global configuration mode.
Step 8	**interface port-channel** *port-channel number*	Enter port-channel interface mode.
Step 9	**shutdown**	Shut down the interface.
Step 10	**no shutdown**	Enable the interface.
Step 11	**end**	Return to privileged EXEC mode.
Step 12	**show l2protocol**	Display the Layer 2 tunnel ports on the switch, including the protocols configured, the thresholds, and the counters.
Step 13	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no switchport mode trunk**, the **no udld enable**, and the **no channel group** *channel-group-number* **mode desirable** interface configuration commands to return the interface to the default settings.

EXAMPLE

This example shows how to configure the customer switch at Site 1. Fast Ethernet interfaces 1, 2, 3, and 4 are set for 802.1Q trunking, UDLD is enabled, EtherChannel group 1 is enabled, and the port channel is shut down and then enabled to activate the EtherChannel configuration.

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet0/2
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet0/3
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet0/4
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface port-channel 1
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Verifying Configuration

Command	Purpose
clear l2protocol-tunnel counters	Clear the protocol counters on Layer 2 protocol tunneling ports.
show l2protocol-tunnel	Display information about Layer 2 protocol tunneling ports.
show errdisable recovery	Verify if the recovery timer from a Layer 2 protocol-tunnel error disable state is enabled.
show l2protocol-tunnel interface *interface-id*	Display information about a specific Layer 2 protocol tunneling port.
show l2protocol-tunnel summary	Display only Layer 2 protocol summary information.

Configuration Example

This example shows how to configure Layer 2 protocol tunneling for CDP, STP, and VTP and to verify the configuration.

```
Switch(config)# interface gigaethernet0/1
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# l2protocol-tunnel stp
Switch(config-if)# l2protocol-tunnel vtp
Switch(config-if)# l2protocol-tunnel shutdown-threshold 1500
Switch(config-if)# l2protocol-tunnel drop-threshold 1000
Switch(config-if)# exit
Switch(config)# l2protocol-tunnel cos 7
Switch(config)# end
Switch# show l2protocol
COS for Encapsulated Packets: 7
Port      Protocol Shutdown  Drop      Encapsulation Decapsulation Drop
                   Threshold Threshold Counter       Counter       Counter
-------   -------- --------- --------- ------------- ------------- -------------
Gi  0/1  cdp           1500      1000 2288          2282          0
          stp           1500      1000 116           13            0
          vtp           1500      1000 3             67            0
          pagp          ----      ---- 0             0             0
          lacp          ----      ---- 0             0             0
          udld          ----      ---- 0             0             0
```

This example shows how to configure the SP edge switch 1 and edge switch 2. VLANs 17, 18, 19, and 20 are the access VLANs, Gigabit Ethernet interfaces 1 and 2 are point-to-point tunnel ports with PAgP and UDLD enabled, the drop threshold is 1000, and Fast Ethernet interface 3 is a trunk port.

SP edge switch 1 configuration:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport access vlan 17
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport access vlan 18
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet0/3
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
```

SP edge switch 2 configuration:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport access vlan 19
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport access vlan 20
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet0/3
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
```

This example shows how to configure the customer switch at Site 1. Fast Ethernet interfaces 1, 2, 3, and 4 are set for 802.1Q trunking, UDLD is enabled, EtherChannel group 1 is enabled, and the port channel is shut down and then enabled to activate the EtherChannel configuration.

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet0/2
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet0/3
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet0/4
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface port-channel 1
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS LAN Switching Command Reference
- Cisco IOS Interface and Hardware Component Command Reference
- High Availability and Redundancy Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520 Switch	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

CHAPTER 11

Configuring STP

This chapter describes how to configure the Spanning Tree Protocol (STP) on port-based VLANs on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*. The switch can use the per-VLAN spanning-tree plus (PVST+) protocol based on the IEEE 802.1D standard and Cisco proprietary extensions, or the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol based on the 802.1w standard. On the switch, STP is enabled by default on network node interfaces (NNIs). It is disabled by default, but can be enabled, on enhanced network interfaces (ENIs). User network interfaces (UNIs) on the switch do not participate in STP. UNIs and ENIs on which STP is not enabled immediately forward traffic when they are brought up.

For information about the Multiple Spanning Tree Protocol (MSTP) and how to map multiple VLANs to the same spanning-tree instance, see Chapter 12, "Configuring MSTP." For information about other spanning-tree features such as Port Fast, root guard, and so forth, see Chapter 13, "Configuring Optional Spanning-Tree Features."

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 11-29.

This chapter includes the following sections:

- Information About Spanning-Tree Features, page 11-1
- Prerequisites, page 11-11
- Guidelines and Limitations, page 11-11
- Default Settings, page 11-12
- Configuring Spanning-Tree Features, page 11-13
- Verifying Configuration, page 11-28
- Configuration Example, page 11-28
- Related Documents, page 11-29
- Feature History, page 11-30

Information About Spanning-Tree Features

- STP Overview, page 11-2
- Spanning-Tree Topology and BPDUs, page 11-3

For configuration information, see the "Guidelines and Limitations" section on page 11-11.

For information about optional spanning-tree features, see Chapter 13, "Configuring Optional Spanning-Tree Features."

STP Overview

STP is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Switches might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network. Spanning-tree 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.

The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology:

- Root—A forwarding port elected for the spanning-tree topology
- Designated—A forwarding port elected for every switched LAN segment
- Alternate—A blocked port providing an alternate path to the root bridge in the spanning tree
- Backup—A blocked port in a loopback configuration

Note Only NNIs and ENIs on which STP has been enabled participate in STP. Active UNIs and ENIs on which STP is not enabled are always in the forwarding state. In this overview, STP ports can be any interfaces on other switches, but only NNIs or STP-enabled ENIs on a Cisco Connected Grid switch.

The switch that has *all* of its ports as the designated role or the backup role is the root switch. The switch that has at least *one* of its ports in the designated role is called the designated switch.

Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switches do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment.

When two ports on a switch are part of a loop, the spanning-tree port priority and path cost settings control which port is put in the forwarding state and which is put in the blocking state. The spanning-tree port priority value represents the location of a port in the network topology and how well it is located to pass traffic. The path cost value represents the media speed.

Note The switch sends keepalive messages (to ensure that the connection is up) only on interfaces that do not have small form-factor pluggable (SFP) modules.

Spanning-Tree Topology and BPDUs

The stable, active spanning-tree topology of a switched network is controlled by these elements:

- The unique bridge ID (switch priority and MAC address) associated with each VLAN on each switch.
- The spanning-tree path cost to the root switch.
- The port identifier (port priority and MAC address) associated with each Layer 2 STP-enabled interface.

When the switches in a network are powered up, each functions as the root switch. Each switch sends a configuration BPDU through all of its ports, or on the Cisco Connected Grid switch, only through the STP-enabled ports. The BPDUs communicate and compute the spanning-tree topology. Each configuration BPDU contains this information:

- The unique bridge ID of the switch that the sending switch identifies as the root switch
- The spanning-tree path cost to the root
- The bridge ID of the sending switch
- Message age
- The identifier of the sending interface
- Values for the hello, forward delay, and max-age protocol timers

When a switch receives a configuration BPDU that contains *superior* information (lower bridge ID, lower path cost, and so forth), it stores the information for that port. If this BPDU is received on the root port of the switch, the switch also forwards it with an updated message to all attached LANs for which it is the designated switch.

If a switch receives a configuration BPDU that contains *inferior* information to that currently stored for that port, it discards the BPDU. If the switch is a designated switch for the LAN from which the inferior BPDU was received, it sends that LAN a BPDU containing the up-to-date information stored for that port. In this way, inferior information is discarded, and superior information is propagated on the network.

A BPDU exchange results in these actions:

- One switch in the network is elected as the root switch (the logical center of the spanning-tree topology in a switched network).

  For each VLAN, the switch with the highest switch priority (the lowest numerical priority value) is elected as the root switch. If all switches are configured with the default priority (32768), the switch with the lowest MAC address in the VLAN becomes the root switch. The switch priority value occupies the most significant bits of the bridge ID, as shown in Table 11-1 on page 11-4.

- A root port is selected for each switch (except the root switch). This port provides the best path (lowest cost) when the switch forwards packets to the root switch.
- The shortest distance to the root switch is calculated for each switch based on the path cost.
- A designated switch for each LAN segment is selected. The designated switch incurs the lowest path cost when forwarding packets from that LAN to the root switch. The port through which the designated switch is attached to the LAN is called the designated port. For the Cisco Connected Grid switch, this only applies to NNIs or to ENIs on which STP has been specifically enabled.

All paths that are not needed to reach the root switch from anywhere in the switched network are placed in the spanning-tree blocking mode.

Bridge ID, Switch Priority, and Extended System ID

The 802.1D standard requires that each switch has an unique bridge identifier (bridge ID), which controls the selection of the root switch. Because each VLAN is considered as a different *logical bridge* with PVST+ and rapid PVST+, the same switch must have as many different bridge IDs as VLANs configured on it. Each VLAN on the switch has a unique 8-byte bridge ID. The two most-significant bytes are used for the switch priority, and the remaining six bytes are derived from the switch MAC address.

The switch supports the 802.1t spanning-tree extensions, and some of the bits previously used for the switch priority are now used as the VLAN identifier. The result is that fewer MAC addresses are reserved for the switch, and a larger range of VLAN IDs can be supported, all while maintaining the uniqueness of the bridge ID. As shown in Table 11-1, the two bytes previously used for the switch priority are reallocated into a 4-bit priority value and a 12-bit extended system ID value equal to the VLAN ID.

Table 11-1 Switch Priority Value and Extended System ID

Switch Priority Value				Extended System ID (Set Equal to the VLAN ID)											
Bit 16	**Bit 15**	**Bit 14**	**Bit 13**	**Bit 12**	**Bit 11**	**Bit 10**	**Bit 9**	**Bit 8**	**Bit 7**	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Spanning tree uses the extended system ID, the switch priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN.

Support for the extended system ID affects how you manually configure the root switch, the secondary root switch, and the switch priority of a VLAN. For example, when you change the switch priority value, you change the probability that the switch will be elected as the root switch. Configuring a higher value decreases the probability; a lower value increases the probability. For more information, see the "Configuring the Root Switch" section on page 11-16, the "Configuring a Secondary Root Switch" section on page 11-19, and the "Configuring the Switch Priority of a VLAN" section on page 11-24.

Spanning-Tree Interface States

Propagation delays can occur when protocol information passes through a switched LAN. As a result, topology changes can take place at different times and at different places in a switched network. When an STP port transitions directly from nonparticipation in the spanning-tree topology to the forwarding state, it can create temporary data loops. Interfaces must wait for new topology information to propagate through the switched LAN before starting to forward frames. They must allow the frame lifetime to expire for forwarded frames that have used the old topology.

Each Layer 2 interface on a switch using spanning tree exists in one of these states:

- Blocking—The interface does not participate in frame forwarding.
- Listening—The first transitional state after the blocking state when the spanning tree determines that the interface should participate in frame forwarding.
- Learning—The interface prepares to participate in frame forwarding.
- Forwarding—The interface forwards frames.
- Disabled—The interface is not participating in spanning tree because of a shutdown port, no link on the port, or no spanning-tree instance running on the port.

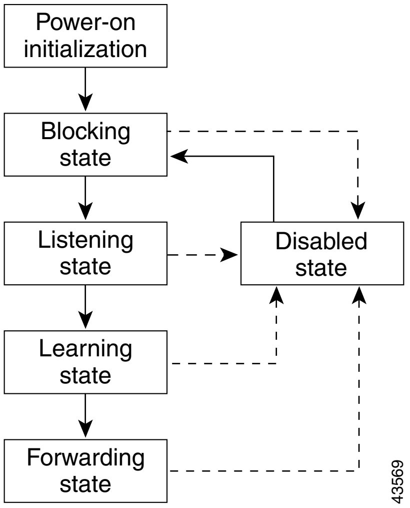
Note On a Cisco Connected Grid switch, UNIs are always in the forwarding state. ENIs in the default STP mode (disabled) are also in forwarding state, but you can enable STP on an ENI.

A port participating in spanning tree moves through these states:

- From initialization to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled

Figure 11-1 illustrates how an interface moves through the states.

Figure 11-1 Spanning-Tree Interface States



When you power up the switch, spanning tree is enabled by default, and every NNI in the Cisco Connected Grid switch (and every ENI on which STP has been enabled), as well as any other port in other switches in the VLAN or network that are participating in spanning tree, goes through the blocking state and the transitory states of listening and learning. Spanning tree stabilizes each interface at the forwarding or blocking state.

Note UNIs are shut down by default, and when they are brought up, they immediately start forwarding traffic. ENIs act the same as UNIs unless you have specifically enabled STP on the port.

When the spanning-tree algorithm places a Layer 2 spanning-tree interface in the forwarding state, this process occurs:

1. The interface is in the listening state while spanning tree waits for protocol information to transition the interface to the blocking state.
2. While spanning tree waits the forward-delay timer to expire, it moves the interface to the learning state and resets the forward-delay timer.
3. In the learning state, the interface continues to block frame forwarding as the switch learns end-station location information for the forwarding database.
4. When the forward-delay timer expires, spanning tree moves the interface to the forwarding state, where both learning and frame forwarding are enabled.

Blocking State

A Layer 2 interface in the blocking state does not participate in frame forwarding. After initialization, a BPDU is sent to each switch interface, or to each switch STP port. A switch initially functions as the root until it exchanges BPDUs with other switches. This exchange establishes which switch in the network is the root or root switch. If there is only one switch in the network, no exchange occurs, the forward-delay timer expires, and the interface moves to the listening state. An interface participating in spanning tree always enters the blocking state after switch initialization.

An interface in the blocking state performs these functions:

- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Does not learn addresses
- Receives BPDUs

Listening State

The listening state is the first state a Layer 2 interface enters after the blocking state. The interface enters this state when the spanning tree decides that the interface should participate in frame forwarding.

An interface in the listening state performs these functions:

- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Does not learn addresses
- Receives BPDUs

Learning State

A Layer 2 interface in the learning state prepares to participate in frame forwarding. The interface enters the learning state from the listening state.

An interface in the learning state performs these functions:

- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Learns addresses
- Receives BPDUs

Forwarding State

A Layer 2 interface in the forwarding state forwards frames. The interface enters the forwarding state from the learning state.

An interface in the forwarding state performs these functions:

- Receives and forwards frames received on the interface
- Forwards frames switched from another interface
- Learns addresses
- Receives BPDUs

Disabled State

A Layer 2 interface in the disabled state does not participate in frame forwarding or in the spanning tree. An interface in the disabled state is nonoperational.

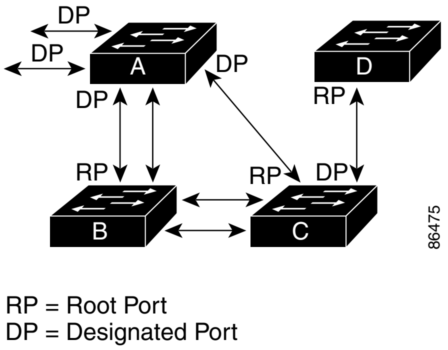
A disabled interface performs these functions:

- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Does not learn addresses
- Does not receive BPDUs

How a Switch or Port Becomes the Root Switch or Root Port

If all switches in a network are enabled with default spanning-tree settings, the switch with the lowest MAC address becomes the root switch. In Figure 11-2, Switch A is elected as the root switch because the switch priority of all the switches is set to the default (32768) and Switch A has the lowest MAC address. However, because of traffic patterns, number of forwarding interfaces, or link types, Switch A might not be the ideal root switch. By increasing the priority (lowering the numerical value) of the ideal switch so that it becomes the root switch, you force a spanning-tree recalculation to form a new topology with the ideal switch as the root.

Figure 11-2 Spanning-Tree Topology



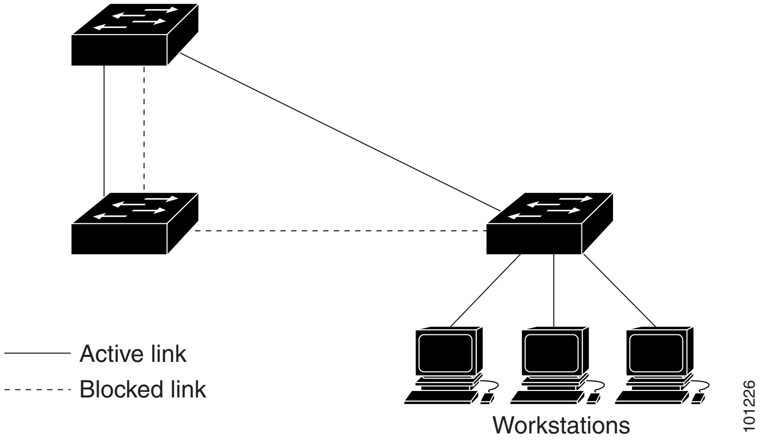
When the spanning-tree topology is calculated based on default parameters, the path between source and destination end stations in a switched network might not be ideal. For instance, connecting higher-speed links to an interface that has a higher number than the root port can cause a root-port change. The goal is to make the fastest link the root port.

For example, assume that one port on Switch B is a Gigabit Ethernet link and that another port on Switch B (a 10/100 link) is the root port. Network traffic might be more efficient over the Gigabit Ethernet link. By changing the spanning-tree port priority on the Gigabit Ethernet port to a higher priority (lower numerical value) than the root port, the Gigabit Ethernet port becomes the new root port.

Spanning Tree and Redundant Connectivity

You can create a redundant backbone with spanning tree by connecting two switch interfaces that are participating in spanning tree to another device or to two different devices, as shown in Figure 11-3. Spanning tree automatically disables one interface but enables it if the other one fails. If one link is high-speed and the other is low-speed, the low-speed link is always disabled. If the speeds are the same, the port priority and port ID are added together, and spanning tree disables the link with the lowest value.

Figure 11-3 Spanning Tree and Redundant Connectivity



You can also create redundant links between switches by using EtherChannel groups. For more information, see the "Configuring EtherChannels and Link State Tracking" chapter in the *High Availability and Redundancy Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.

Spanning-Tree Address Management

802.1D specifies 17 multicast addresses, ranging from 0x00180C2000000 to 0x0180C2000010, to be used by different bridge protocols. These addresses are static addresses that cannot be removed.

Regardless of the spanning-tree state, each switch receives but does not forward packets destined for addresses between 0x0180C2000000 and 0x0180C200000F.

If spanning tree is enabled, the CPU on the switch receives packets destined for 0x0180C2000000 and 0x0180C2000010. If spanning tree is disabled, the switch forwards those packets as unknown multicast addresses.

Accelerated Aging to Retain Connectivity

The default for aging dynamic addresses is 5 minutes, the default setting of the **mac address-table aging-time** global configuration command. However, a spanning-tree reconfiguration can cause many station locations to change. Because these stations could be unreachable for 5 minutes or more during a reconfiguration, the address-aging time is accelerated so that station addresses can be dropped from the address table and then relearned. The accelerated aging is the same as the forward-delay parameter value (**spanning-tree vlan** *vlan-id* **forward-time** *seconds* global configuration command) when the spanning tree reconfigures.

Because each VLAN is a separate spanning-tree instance, the switch accelerates aging on a per-VLAN basis. A spanning-tree reconfiguration on one VLAN can cause the dynamic addresses learned on that VLAN to be subject to accelerated aging. Dynamic addresses on other VLANs can be unaffected and remain subject to the aging interval entered for the switch.

Spanning-Tree Modes and Protocols

The switch NNIs and ENIs with STP enabled support these spanning-tree modes and protocols:

- PVST+—This spanning-tree mode is based on the 802.1D standard and Cisco proprietary extensions. It is the default spanning-tree mode used on most Ethernet port-based VLANs. The PVST+ runs on each VLAN on the switch up to the maximum supported, ensuring that each has a loop-free path through the network.

  The PVST+ provides Layer 2 load balancing for the VLAN on which it runs. You can create different logical topologies by using the VLANs on your network to ensure that all of your links are used but that no one link is oversubscribed. Each instance of PVST+ on a VLAN has a single root switch. This root switch propagates the spanning-tree information associated with that VLAN to all other switches in the network. Because each switch has the same information about the network, this process ensures that the network topology is maintained.

- Rapid PVST+—This spanning-tree mode is the same as PVST+ except that is uses a rapid convergence based on the 802.1w standard. This is the default spanning-tree mode for the Cisco Connected Grid switch NNIs. Rapid PVST+ is compatible with PVST+. To provide rapid convergence, the rapid PVST+ immediately deletes dynamically learned MAC address entries on a per-port basis upon receiving a topology change. By contrast, PVST+ uses a short aging time for dynamically learned MAC address entries.

The rapid PVST+ uses the same configuration as PVST+ (except where noted), and the switch needs only minimal extra configuration. The benefit of rapid PVST+ is that you can migrate a large PVST+ install base to rapid PVST+ without having to learn the complexities of the MSTP configuration and without having to reprovision your network. In rapid-PVST+ mode, each VLAN runs its own spanning-tree instance up to the maximum supported.

- MSTP—This spanning-tree mode is based on the 802.1s standard. You can map multiple VLANs to the same spanning-tree instance, which reduces the number of spanning-tree instances required to support a large number of VLANs. The MSTP runs on top of the RSTP (based on 802.1w), which provides for rapid convergence of the spanning tree by eliminating the forward delay and by quickly transitioning root ports and designated ports to the forwarding state. You cannot run MSTP without RSTP.

  The most common initial deployment of MSTP is in the backbone and distribution layers of a Layer 2 switched network. For more information, see Chapter 12, "Configuring MSTP."

For information about the number of supported spanning-tree instances, see the next section.

Supported Spanning-Tree Instances

In PVST+ or rapid-PVST+ mode, the switch supports up to 128 spanning-tree instances.

In MSTP mode, the switch supports up to 65 MST instances. The number of VLANs that can be mapped to a particular MST instance is unlimited.

Spanning-Tree Interoperability and Backward Compatibility

Table 11-2 lists the interoperability and compatibility among the supported spanning-tree modes in a network.

Table 11-2 PVST+, MSTP, and Rapid-PVST+ Interoperability

	PVST+	MSTP	Rapid PVST+
PVST+	Yes	Yes (with restrictions)	Yes (reverts to PVST+)
MSTP	Yes (with restrictions)	Yes	Yes (reverts to PVST+)
Rapid PVST+	Yes (reverts to PVST+)	Yes (reverts to PVST+)	Yes

In a mixed MSTP and PVST+ network, the common spanning-tree (CST) root must be inside the MST backbone, and a PVST+ switch cannot connect to multiple MST regions.

When a network contains switches running rapid PVST+ and switches running PVST+, we recommend that the rapid-PVST+ switches and PVST+ switches be configured for different spanning-tree instances. In the rapid-PVST+ spanning-tree instances, the root switch must be a rapid-PVST+ switch. In the PVST+ instances, the root switch must be a PVST+ switch. The PVST+ switches should be at the edge of the network.

STP and IEEE 802.1Q Trunks

The 802.1Q standard for VLAN trunks imposes some limitations on the spanning-tree strategy for a network. The standard requires only one spanning-tree instance for *all* VLANs allowed on the trunks. However, in a network of Cisco switches connected through 802.1Q trunks, the switches maintain one spanning-tree instance for *each* VLAN allowed on the trunks.

When you connect a Cisco switch to a non-Cisco device through an 802.1Q trunk, the Cisco switch uses PVST+ to provide spanning-tree interoperability. If rapid PVST+ is enabled, the switch uses it instead of PVST+. The switch combines the spanning-tree instance of the 802.1Q VLAN of the trunk with the spanning-tree instance of the non-Cisco 802.1Q switch.

However, all PVST+ or rapid-PVST+ information is maintained by Cisco switches separated by a cloud of non-Cisco 802.1Q switches. The non-Cisco 802.1Q cloud separating the Cisco switches is treated as a single trunk link between the switches.

PVST+ is automatically enabled on 802.1Q trunks, and no user configuration is required. The external spanning-tree behavior on access ports is not affected by PVST+.

For more information on 802.1Q trunks, see Chapter 3, “Configuring VLANs.”

Prerequisites

- Be familiar with the information in the “Information About Spanning-Tree Features” section on page 11-1 and “Guidelines and Limitations” section on page 11-11.
- Ensure that your network strategy and planning for your network are complete.

Guidelines and Limitations

If more VLANs are defined than there are spanning-tree instances, you can enable PVST+ or rapid PVST+ on STP ports in only 128 VLANs on the switch. The remaining VLANs operate with spanning tree disabled. However, you can map multiple VLANs to the same spanning-tree instances by using MSTP. For more information, see Chapter 12, “Configuring MSTP.”

If 128 instances of spanning tree are already in use, you can disable spanning tree on STP ports in one of the VLANs and then enable it on the VLAN where you want it to run. Use the **no spanning-tree vlan** *vlan-id* global configuration command to disable spanning tree on a specific VLAN, and use the **spanning-tree vlan** *vlan-id* global configuration command to enable spanning tree on the desired VLAN.

⚠ **Caution** Switches that are not running spanning tree still forward BPDUs that they receive so that the other switches on the VLAN that have a running spanning-tree instance can break loops. Therefore, spanning tree must be running on enough switches to break all the loops in the network; for example, at least one switch on each loop in the VLAN must be running spanning tree. It is not absolutely necessary to run spanning tree on all switches in the VLAN. However, if you are running spanning tree only on a minimal set of switches, an incautious change to the network that introduces another loop into the VLAN can result in a broadcast storm.

If you have already used all available spanning-tree instances on your switch, adding another VLAN creates a VLAN that is not running spanning tree on that switch. If you have the default allowed list on the trunk ports of that switch, the new VLAN is carried on all trunk ports. Depending on the topology of the network, this could create a loop in the new VLAN that will not be broken, particularly if there are several adjacent switches that have all run out of spanning-tree instances. You can prevent this possibility by setting up allowed lists on the trunk ports of switches that have used up their allocation of spanning-tree instances. Setting up allowed lists is not necessary in many cases and can make it more labor-intensive to add another VLAN to the network.

Spanning-tree commands control the configuration of VLAN spanning-tree instances. You create a spanning-tree instance when you assign an STP port (an NNI or ENI with STP enabled) to a VLAN. The spanning-tree instance is removed when the last port is moved to another VLAN. You can configure switch and port parameters before a spanning-tree instance is created; these parameters are applied when the spanning-tree instance is created.

The switch supports PVST+, rapid PVST+, and MSTP, but only one version can be active at any time. (For example, all VLANs run PVST+, all VLANs run rapid PVST+, or all VLANs run MSTP.) For information about the different spanning-tree modes and how they interoperate, see the "Spanning-Tree Interoperability and Backward Compatibility" section on page 11-10.

⚠ **Caution** Loop guard works only on point-to-point links. We recommend that each end of the link has a directly connected device that is running STP.

On the switch, when 1-to-1 VLAN mapping is enabled on an NNI or on an ENI on which STP is enabled, the STP instance applies to the service provider VLAN (S-VLAN) within the switch.

Default Settings

Feature	**Default Setting**
Enable state	Enabled on NNIs in VLAN 1. Disabled on ENIs. (Not supported on UNIs) For more information, see the "Supported Spanning-Tree Instances" section on page 11-10.
Spanning-tree mode	Rapid PVST+ Rapid PVST+ interoperates with PVST and PVST+. MSTP is disabled.
Switch priority	32768.
Spanning-tree port priority (configurable on a per-interface basis)	128.
Spanning-tree port cost (configurable on a per-interface basis)	1000 Mbps: 4. 100 Mbps: 19. 10 Mbps: 100.
Spanning-tree VLAN port priority (configurable on a per-VLAN basis)	128.

Feature	Default Setting
Spanning-tree VLAN port cost (configurable on a per-VLAN basis)	1000 Mbps: 4. 100 Mbps: 19. 10 Mbps: 100.
Spanning-tree timers	Hello time: 2 seconds. Forward-delay time: 15 seconds. Maximum-aging time: 20 seconds.

Configuring Spanning-Tree Features

This section includes the following topics:

- Enabling Spanning Tree on an ENI, page 11-13 (required)
- Changing the Spanning-Tree Mode, page 11-14
- Disabling Spanning Tree, page 11-16 (optional)
- Configuring the Root Switch, page 11-16 (optional)
- Configuring a Secondary Root Switch, page 11-19 (optional)
- Configuring Port Priority, page 11-21 (optional)
- Configuring Path Cost, page 11-22 (optional)
- Configuring the Switch Priority of a VLAN, page 11-24 (optional)
- Configuring Spanning-Tree Timers, page 11-25 (optional)

Enabling Spanning Tree on an ENI

By default, spanning tree is enabled on all NNIs on the switch and disabled on ENIs. Follow this procedure to enable spanning tree on an ENI.

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 11-11.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify a UNI or ENI interface to configure, and enter interface configuration mode.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled.
Step 4	**port-type eni**	Configure the port as an ENI (if not already configured).

	Command	Purpose
Step 5	**spanning-tree**	Enable spanning tree on the interface. The interface will belong to the switch spanning tree instance along with NNIs in the VLAN. **Note** This command is visible only on ENIs.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show spanning-tree interface** *interface-id*	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable spanning tree on an ENI, enter the **no spanning-tree** interface command.

EXAMPLE

This example enables spanning tree on an ENI interface.

```
Switch(config)# interface fastethernet 3/1
Switch(config-if)# no shutdown
Switch(config-if)# port-type eni
Switch(config-if)# spanning tree
Switch(config-if)# end
```

Changing the Spanning-Tree Mode

The switch supports three spanning-tree modes: PVST+, rapid PVST+, or MSTP. By default, the switch runs the rapid PVST+ protocol on all NNIs and ENIs on which spanning tree is enabled. If you want to enable a mode that is different from the default mode, this procedure is required.

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 11-11.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree mode** {**pvst** | **mst** | **rapid-pvst**}	Configure a spanning-tree mode on STP ports on the switch. • Specify **pvst** to enable PVST+. • Specify **mst** to enable MSTP (and RSTP). For more configuration steps, see Chapter 12, "Configuring MSTP." • Specify **rapid-pvst** to enable rapid PVST+ (the default setting).

	Command	Purpose
Step 3	**interface** *interface-id*	(Recommended only for rapid-PVST+ mode) Specify an STP port to configure, and enter interface configuration mode. Valid interfaces include physical NNIs or ENIs with spanning tree enabled, VLANs, and NNI or ENI port channels. The VLAN ID range is 1 to 4094. The port-channel range is 1 to 48. **Note** If a physical interface is a UNI, before attempting to configure it as a spanning-tree link, you must enter the **port-type nni** interface configuration command or configure the port as an ENI and enable spanning tree on the port. See "Enabling Spanning Tree on an ENI" section on page 11-13. If the interface is a VLAN, only ports with spanning tree enabled in the VLAN will run spanning tree. If the interface is a port channel, all members of the port channel must be NNIs or ENIs with spanning tree enabled.
Step 4	**spanning-tree link-type point-to-point**	(Recommended only for rapid-PVST+ mode) Specify that the link type for this port is point-to-point. If you connect this port to a remote port through a point-to-point link and the local port becomes a designated port, the switch negotiates with the remote port and rapidly changes the local port to the forwarding state.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**clear spanning-tree detected-protocols**	(Recommended only for rapid-PVST+ mode) If any port on the switch running spanning tree is connected to a port on a legacy 802.1D switch, restart the protocol migration process on the entire switch. This step is optional if the designated switch detects that this switch is running rapid PVST+.
Step 7	**show spanning-tree summary** and **show spanning-tree interface** *interface-id*	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no spanning-tree mode** global configuration command. To return the port to its default spanning-tree mode setting, use the **no spanning-tree link-type** interface configuration command.

EXAMPLE

This example shows how to enable MST:

```
Switch(config)# spanning-tree mode mst
```

Disabling Spanning Tree

Spanning tree is enabled by default on all NNIs in VLAN 1 and in all newly created VLANs up to the spanning-tree limit specified in the "Supported Spanning-Tree Instances" section on page 11-10. Spanning tree is disabled on ENIs on the switch but can be enabled on a per-interface basis.

Caution When spanning tree is disabled and loops are present in the topology, excessive traffic and indefinite packet duplication can drastically reduce network performance.

BEFORE YOU BEGIN

Disable spanning tree only if you are sure there are no loops in the network topology.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no spanning-tree vlan** *vlan-id*	For *vlan-id*, the range is 1 to 4094.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree vlan** *vlan-id*	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To re-enable spanning-tree, use the **spanning-tree vlan** *vlan-id* global configuration command.

EXAMPLE

This example disables spanning tree for VLAN 200:

```
Switch(config)# no spanning tree vlan 200
Switch(config)# end
```

Configuring the Root Switch

The switch maintains a separate spanning-tree instance for each active VLAN configured on it. A bridge ID, consisting of the switch priority and the switch MAC address, is associated with each instance. For each VLAN, the switch with the lowest bridge ID becomes the root switch for that VLAN.

To configure a switch to become the root for the specified VLAN, use the **spanning-tree vlan** *vlan-id* **root** global configuration command to modify the switch priority from the default value (32768) to a significantly lower value. When you enter this command, the software checks the switch priority of the root switches for each VLAN. Because of the extended system ID support, the switch sets its own priority for the specified VLAN to 24576 if this value will cause this switch to become the root for the specified VLAN.

If any root switch for the specified VLAN has a switch priority lower than 24576, the switch sets its own priority for the specified VLAN to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value as shown in Table 11-1 on page 11-4.)

Note The **spanning-tree vlan** *vlan-id* **root** global configuration command fails if the value necessary to be the root switch is less than 1.

If your network consists of switches that both do and do not support the extended system ID, it is unlikely that the switch with the extended system ID support will become the root switch. The extended system ID increases the switch priority value every time the VLAN number is greater than the priority of the connected switches running older software.

Note After configuring the switch as the root switch, we recommend that you avoid manually configuring the hello time, forward-delay time, and maximum-age time through the **spanning-tree vlan** *vlan-id* **hello-time**, **spanning-tree vlan** *vlan-id* **forward-time**, and the **spanning-tree vlan** *vlan-id* **max-age** global configuration commands.

Follow this procedure to configure a switch to become the root for the specified VLAN. This procedure is optional.

BEFORE YOU BEGIN

- The root switch for each spanning-tree instance should be a backbone or distribution switch. Do not configure an access switch as the spanning-tree primary root.
- Use the **diameter** keyword to specify the Layer 2 network diameter (that is, the maximum number of switch hops between any two end stations in the Layer 2 network). When you specify the network diameter, the switch automatically sets an optimal hello time, forward-delay time, and maximum-age time for a network of that diameter, which can significantly reduce the convergence time. You can use the **hello** keyword to override the automatically calculated hello time.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree vlan** *vlan-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	Configure a switch to become the root for the specified VLAN. • For *vlan-id*, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. • (Optional) For **diameter** *net-diameter*, specify the maximum number of switches between any two end stations. The range is 2 to 7. • (Optional) For **hello-time** *seconds*, specify the interval in seconds between the generation of configuration messages by the root switch. The range is 1 to 10; the default is 2.
Step 3	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 4	**show spanning-tree detail**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no spanning-tree vlan** *vlan-id* **root** global configuration command.

EXAMPLE

This example shows how to configure a switch as the root bridge for VLAN 10, with a network diameter of 4:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 10 root primary diameter 4
Switch(config)# end
Switch#
```

This example shows how the configuration changes when a switch becomes a spanning tree root. This is the configuration before the switch becomes the root for VLAN 1:

```
Switch# show spanning-tree vlan 1
VLAN1 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 32768, address 0030.94fc.0a00
Configured hello time 2, max age 20, forward delay 15
Current root has priority 32768, address 0001.6445.4400
Root port is 323 (FastEthernet6/3), cost of root path is 19
Topology change flag not set, detected flag not set
Number of topology changes 2 last change occurred 00:02:19 ago
       from FastEthernet6/1
Times: hold 1, topology change 35, notification 2
       hello 2, max age 20, forward delay 15
Timers:hello 0, topology change 0, notification 0, aging 300

Port 323 (FastEthernet6/3) of VLAN1 is forwarding
    Port path cost 19, Port priority 128, Port Identifier 129.67.
    Designated root has priority 32768, address 0001.6445.4400
    Designated bridge has priority 32768, address 0001.6445.4400
    Designated port id is 129.67, designated path cost 0
    Timers:message age 2, forward delay 0, hold 0
    Number of transitions to forwarding state:1
    BPDU:sent 3, received 91
Port 324 (FastEthernet6/4) of VLAN1 is blocking
    Port path cost 19, Port priority 128, Port Identifier 129.68.
    Designated root has priority 32768, address 0001.6445.4400
    Designated bridge has priority 32768, address 0001.6445.4400
    Designated port id is 129.68, designated path cost 0
    Timers:message age 2, forward delay 0, hold 0
    Number of transitions to forwarding state:0
    BPDU:sent 1, received 89
```

Now, you can set the switch as the root:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 1 root primary
    VLAN 1 bridge priority set to 8192
    VLAN 1 bridge max aging time unchanged at 20
    VLAN 1 bridge hello time unchanged at 2
    VLAN 1 bridge forward delay unchanged at 15
Switch(config)# end
```

This is the configuration after the switch becomes the root:

```
Switch# show spanning-tree vlan 1
VLAN1 is executing the ieee compatible Spanning Tree protocol
    Bridge Identifier has priority 8192, address 0030.94fc.0a00
    Configured hello time 2, max age 20, forward delay 15
    We are the root of the spanning tree
    Topology change flag set, detected flag set
    Number of topology changes 3 last change occurred 00:00:09 ago
    Times: hold 1, topology change 35, notification 2
    hello 2, max age 20, forward delay 15
    Timers:hello 0, topology change 25, notification 0, aging 15
Port 323 (FastEthernet6/3) of VLAN1 is forwarding
    Port path cost 19, Port priority 128, Port Identifier 129.67.
    Designated root has priority 8192, address 0030.94fc.0a00
    Designated bridge has priority 8192, address 0030.94fc.0a00
    Designated port id is 129.67, designated path cost 0
    Timers:message age 0, forward delay 0, hold 0
    Number of transitions to forwarding state:1
    BPDU:sent 9, received 105
Port 324 (FastEthernet6/4) of VLAN1 is listening
    Port path cost 19, Port priority 128, Port Identifier 129.68.
    Designated root has priority 8192, address 0030.94fc.0a00
    Designated bridge has priority 8192, address 0030.94fc.0a00
    Designated port id is 129.68, designated path cost 0
    Timers:message age 0, forward delay 5, hold 0
    Number of transitions to forwarding state:0
    BPDU:sent 6, received 102
Switch#
```

Note Because the bridge priority is now set at 8192, this switch becomes the root of the spanning tree.

Configuring a Secondary Root Switch

When you configure a switch as the secondary root, the switch priority is modified from the default value (32768) to 28672. The switch is then likely to become the root switch for the specified VLAN if the primary root switch fails. This is assuming that the other network switches use the default switch priority of 32768 and therefore are unlikely to become the root switch.

You can execute this command on more than one switch to configure multiple backup root switches. Use the same network diameter and hello-time values that you used when you configured the primary root switch with the **spanning-tree vlan** *vlan-id* **root primary** global configuration command.

Note After configuring the switch as the root switch, we recommend that you avoid manually configuring the hello time, forward-delay time, and maximum-age time through the **spanning-tree vlan** *vlan-id* **hello-time**, **spanning-tree vlan** *vlan-id* **forward-time**, and the **spanning-tree vlan** *vlan-id* **max-age** global configuration commands.

Follow this procedure to configure a switch to become the secondary root for the specified VLAN. This procedure is optional.

BEFORE YOU BEGIN

Use the **diameter** keyword to specify the Layer 2 network diameter (that is, the maximum number of switch hops between any two end stations in the Layer 2 network). When you specify the network diameter, the switch automatically sets an optimal hello time, forward-delay time, and maximum-age time for a network of that diameter, which can significantly reduce the convergence time. You can use the **hello** keyword to override the automatically calculated hello time.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree vlan** *vlan-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	Configure a switch to become the secondary root for the specified VLAN. • For *vlan-id*, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. • (Optional) For **diameter** *net-diameter*, specify the maximum number of switches between any two end stations. The range is 2 to 7. • (Optional) For **hello-time** *seconds*, specify the interval in seconds between the generation of configuration messages by the root switch. The range is 1 to 10; the default is 2. Use the same network diameter and hello-time values that you used when configuring the primary root switch. See the "Configuring the Root Switch" section on page 11-16.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree detail**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no spanning-tree vlan** *vlan-id* **root** global configuration command.

EXAMPLE

This example shows how to configure the switch as the secondary root switch for VLAN 10, with a network diameter of 4:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 10 root secondary diameter 4
    VLAN 10 bridge priority set to 16384
    VLAN 10 bridge max aging time set to 14
    VLAN 10 bridge hello time unchanged at 2
    VLAN 10 bridge forward delay set to 10
Switch(config)# end
Switch#
```

Configuring Port Priority

If a loop occurs, spanning tree uses the port priority when selecting a spanning-tree port to put into the forwarding state. You can assign higher priority values (lower numerical values) to ports that you want selected first and lower priority values (higher numerical values) to ones that you want selected last. If all spanning-tree ports have the same priority value, spanning tree puts the port with the lowest interface number in the forwarding state and blocks the other interfaces.

Follow this procedure to configure the port priority of a spanning-tree port. This procedure is optional.

BEFORE YOU BEGIN

- If a physical interface is a UNI, before attempting to configure it as a spanning-tree link, you must enter the **port-type nni** interface configuration command or configure the port as an ENI and enable spanning tree on the port. See "Enabling Spanning Tree on an ENI" section on page 11-13.
- If the interface is a VLAN, only ports with spanning tree enabled in the VLAN will run spanning tree.
- If the interface is a port channel, all members of the port channel must be NNIs or ENIs with spanning tree enabled.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify an interface to configure, and enter interface configuration mode.
Step 3	**spanning-tree port-priority** *priority*	Configure the port priority for the spanning-tree port. For *priority*, the range is 0 to 240, in increments of 16; the default is 128. Valid values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority.
Step 4	**spanning-tree vlan** *vlan-id* **port-priority** *priority*	Configure the port priority for a VLAN. • For *vlan-id*, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. • For *priority*, the range is 0 to 240, in increments of 16; the default is 128. Valid values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority.
Step 5	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 6	**show spanning-tree interface** *interface-id* or **show spanning-tree vlan** *vlan-id*	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note The **show spanning-tree interface** *interface-id* privileged EXEC command displays information only if the port is in a link-up operative state. Otherwise, you can use the **show running-config interface** privileged EXEC command to confirm the configuration.

To return to the default spanning-tree setting, use the **no spanning-tree** [**vlan** *vlan-id*] **port-priority** interface configuration command. For information on how to configure load sharing on trunk ports by using spanning-tree port priorities, see the "Configuring Trunk Ports for Load Sharing" section on page 4-7.

EXAMPLE

This example shows how to configure the spanning tree port priority of a Fast Ethernet interface:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/8
Switch(config-if)# spanning-tree port-priority 100
Switch(config-if)# end
Switch#
```

Configuring Path Cost

The spanning-tree path cost default value is derived from the media speed of an interface (port running spanning tree or port channel of multiple ports running spanning tree). If a loop occurs, spanning tree uses cost when selecting an interface to put in the forwarding state. You can assign lower cost values to interfaces that you want selected first and higher cost values that you want selected last. If all NNIs (or port channels) have the same cost value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

Follow this procedure to configure the cost of an interface. This procedure is optional.

BEFORE YOU BEGIN

See the "Default Settings" section on page 11-12 for the default path cost values for the interface media speeds.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify an interface to configure, and enter interface configuration mode. Valid interfaces include physical NNIs or ENIs with STP enabled and port-channel logical interfaces (**port-channel** *port-channel-number*) that contain only NNIs or STP-enabled ENIs.
Step 3	**spanning-tree cost** *cost*	Configure the cost for an interface. If a loop occurs, spanning tree uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission. For *cost*, the range is 1 to 200000000; the default value is derived from the media speed of the interface.
Step 4	**spanning-tree vlan** *vlan-id* **cost** *cost*	Configure the cost for a VLAN. If a loop occurs, spanning tree uses the path cost when selecting a spanning-tree port to place into the forwarding state. A lower path cost represents higher-speed transmission. • For *vlan-id*, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. • For *cost*, the range is 1 to 200000000; the default value is derived from the media speed of the interface.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show spanning-tree interface** *interface-id* or **show spanning-tree vlan** *vlan-id*	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note The **show spanning-tree interface** *interface-id* privileged EXEC command displays information only for ports that are in a link-up operative state. Otherwise, you can use the **show running-config** privileged EXEC command to confirm the configuration.

To return to the default setting, use the **no spanning-tree** [**vlan** *vlan-id*] **cost** interface configuration command. For information on how to configure load sharing on trunk ports by using spanning-tree path costs, see the "Configuring Trunk Ports for Load Sharing" section on page 4-7.

EXAMPLE

This example shows how to change the spanning tree port cost of a Fast Ethernet interface:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/8
Switch(config-if)# spanning-tree cost 18
Switch(config-if)# end
Switch#
```

Configuring the Switch Priority of a VLAN

You can configure the switch priority and make it more likely that the switch will be chosen as the root switch. This procedure is optional.

BEFORE YOU BEGIN

Exercise care when using this command. For most situations, we recommend that you use the **spanning-tree vlan** *vlan-id* **root primary** and the **spanning-tree vlan** *vlan-id* **root secondary** global configuration commands to modify the switch priority.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree vlan** *vlan-id* **priority** *priority*	Configure the switch priority of a VLAN. • For *vlan-id*, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. • For *priority*, the range is 0 to 61440 in increments of 4096; the default is 32768. The lower the number, the more likely the switch will be chosen as the root switch. Valid priority values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree vlan** *vlan-id*	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no spanning-tree vlan** *vlan-id* **priority** global configuration command.

EXAMPLE

This example shows how to configure the bridge priority of VLAN 200 to 33,792:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 200 priority 33792
Switch(config)# end
Switch#
```

Configuring Spanning-Tree Timers

Table 11-3 describes the timers that affect the entire spanning-tree performance.

Table 11-3 Spanning-Tree Timers

Variable	Description
Hello timer	Controls how often the switch broadcasts hello messages to other switches.
Forward-delay timer	Controls how long each of the listening and learning states last before the STP port begins forwarding.
Maximum-age timer	Controls the amount of time the switch stores protocol information received on an STP port.

The sections that follow provide the configuration steps.

Configuring the Hello Time

You can configure the interval between the generation of configuration messages by the root switch by changing the hello time. This procedure is optional.

BEFORE YOU BEGIN

Exercise care when using this command. For most situations, we recommend that you use the **spanning-tree vlan** *vlan-id* **root primary** and the **spanning-tree vlan** *vlan-id* **root secondary** global configuration commands to modify the hello time.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree vlan** *vlan-id* **hello-time** *seconds*	Configure the hello time of a VLAN. The hello time is the interval between the generation of configuration messages by the root switch. These messages mean that the switch is alive. • For *vlan-id*, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. • For *seconds*, the range is 1 to 10; the default is 2.
Step 3	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 4	**show spanning-tree vlan** *vlan-id*	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no spanning-tree vlan** *vlan-id* **hello-time** global configuration command.

EXAMPLE

This example shows how to configure the hello time for VLAN 200 to 7 seconds:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 200 hello-time 7
Switch(config)# end
Switch#
```

Configuring the Forward Delay Time for a VLAN

This procedure is optional.

BEFORE YOU BEGIN

Exercise care when configuring forward delay time. In most cases, we recommend that you use the **spanning-tree vlan** *vlan_ID* **root primary** and the **spanning-tree vlan** *vlan_ID* **root secondary** commands to modify the forward delay time.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree vlan** *vlan-id* **forward-time** *seconds*	Configure the forward delay time of a VLAN. The forward delay time is the number of seconds a spanning-tree port waits before changing from its spanning-tree learning and listening states to the forwarding state. • For *vlan-id*, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. • For *seconds*, the range is 4 to 30; the default is 15.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree vlan** *vlan-id*	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no spanning-tree vlan** *vlan-id* **forward-time** global configuration command.

EXAMPLE

This example shows how to configure the forward delay time for VLAN 200 to 21 seconds:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 200 forward-time 21
Switch(config)# end
Switch#
```

Configuring the Maximum-Aging Time for a VLAN

This procedure is optional.

BEFORE YOU BEGIN

Exercise care when configuring aging time. In most cases, we recommend that you use the **spanning-tree vlan** *vlan_ID* **root primary** and the **spanning-tree vlan** *vlan_ID* **root secondary** commands to modify the maximum aging time.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree vlan** *vlan-id* **max-age** *seconds*	Configure the maximum-aging time of a VLAN. The maximum-aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration. • For *vlan-id*, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. • For *seconds*, the range is 6 to 40; the default is 20.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree vlan** *vlan-id*	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no spanning-tree vlan** *vlan-id* **max-age** global configuration command.

EXAMPLE

This example shows how to configure the maximum aging time for VLAN 200 to 36 seconds:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 200 max-age 36
Switch(config)# end
Switch#
```

Verifying Configuration

Command	Purpose
show spanning-tree active	Display spanning-tree information only on active spanning-tree interfaces.
show spanning-tree detail	Display a detailed summary of interface information.
show spanning-tree interface *interface-id*	Display spanning-tree information for the specified spanning-tree interface.
show spanning-tree summary [**totals**]	Display a summary of interface states or displays the total lines of the STP state section.

You can clear spanning-tree counters by using the **clear spanning-tree** [**interface** *interface-id*] privileged EXEC command.

Configuration Example

This example enables spanning tree on an ENI interface.

```
Switch(config)# interface fastethernet 3/1
Switch(config-if)# no shutdown
Switch(config-if)# port-type eni
Switch(config-if)# spanning tree
Switch(config-if)# end
```

This example shows how to enable MST:

```
Switch(config)# spanning-tree mode mst
```

This example disables spanning tree for VLAN 200:

```
Switch(config)# no spanning tree vlan 200
Switch(config)# end
```

This example shows how to configure a switch as the root bridge for VLAN 10, with a network diameter of 4:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 10 root primary diameter 4
Switch(config)# end
Switch#
```

This example shows how to configure the switch as the secondary root switch for VLAN 10, with a network diameter of 4:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 10 root secondary diameter 4
    VLAN 10 bridge priority set to 16384
    VLAN 10 bridge max aging time set to 14
    VLAN 10 bridge hello time unchanged at 2
    VLAN 10 bridge forward delay set to 10
Switch(config)# end
Switch#
```

This example shows how to configure the spanning tree port priority of a Fast Ethernet interface:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/8
Switch(config-if)# spanning-tree port-priority 100
Switch(config-if)# end
Switch#
```

This example shows how to change the spanning tree port cost of a Fast Ethernet interface:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/8
Switch(config-if)# spanning-tree cost 18
Switch(config-if)# end
Switch#
```

This example shows how to configure the bridge priority of VLAN 200 to 33,792:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 200 priority 33792
Switch(config)# end
Switch#
```

This example shows how to configure the hello time for VLAN 200 to 7 seconds:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 200 hello-time 7
Switch(config)# end
Switch#
```

This example shows how to configure the forward delay time for VLAN 200 to 21 seconds:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 200 forward-time 21
Switch(config)# end
Switch#
```

This example shows how to configure the maximum aging time for VLAN 200 to 36 seconds:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 200 max-age 36
Switch(config)# end
Switch#
```

Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS LAN Switching Command Reference
- High Availability and Redundancy Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520 Switch	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

CHAPTER 12

Configuring MSTP

This chapter describes how to configure the Cisco implementation of the IEEE 802.1s Multiple STP (MSTP) on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*. User network interfaces (UNIs) on the switch do not participate in STP and immediately forward traffic when they are brought up. STP is enabled by default on network node interfaces (NNIs), and can be also be enabled on enhanced network interfaces (ENIs). If STP is not enabled on an ENI, the interface always forwards traffic.

Note The multiple spanning-tree (MST) implementation is a pre-standard implementation. It is based on the draft version of the IEEE standard.

The MSTP enables multiple VLANs to be mapped to the same spanning-tree instance, thereby reducing the number of spanning-tree instances needed to support a large number of VLANs. The MSTP provides for multiple forwarding paths for data traffic and enables load balancing. It improves the fault tolerance of the network because a failure in one instance (forwarding path) does not affect other instances (forwarding paths). The most common initial deployment of MSTP is in the backbone and distribution layers of a Layer 2 switched network. This deployment provides the highly available network required in a service-provider environment.

When the switch is in MST mode, the Rapid Spanning Tree Protocol (RSTP), which is based on 802.1w, is automatically enabled. The RSTP provides rapid convergence of the spanning tree through explicit handshaking that eliminates the 802.1D forwarding delay and quickly transitions root ports and designated ports to the forwarding state.

Both MSTP and RSTP improve the spanning-tree operation and maintain backward compatibility with equipment that is based on the (original) 802.1D spanning tree, with existing Cisco-proprietary Multiple Instance STP (MISTP), and with existing Cisco per-VLAN spanning-tree plus (PVST+) and rapid per-VLAN spanning-tree plus (rapid PVST+). For information about PVST+ and rapid PVST+, see Chapter 11, "Configuring STP." For information about other spanning-tree features such as Port Fast, UplinkFast, root guard, and so forth, see Chapter 13, "Configuring Optional Spanning-Tree Features."

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 12-32.

Information About MSTP

MSTP, which uses RSTP for rapid convergence, enables VLANs to be grouped 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.

For configuration information, see the “Guidelines and Limitations” section on page 12-14.

Multiple Spanning-Tree Regions

For switches to participate in multiple spanning-tree (MST) instances, you must consistently configure the switches with the same MST configuration information. A collection of interconnected switches that have the same MST configuration comprises an MST region as shown in Figure 12-1 on page 12-4.

The MST configuration controls to which MST region each switch belongs. The configuration includes the name of the region, the revision number, and the MST VLAN-to-instance assignment map. You configure the switch for a region by using the **spanning-tree mst configuration** global configuration command, after which the switch enters MST configuration mode. From this mode, you can map VLANs to an MST instance by using the **instance** MST configuration command, specify the region name by using the **name** MST configuration command, and set the revision number by using the **revision** MST configuration command.

A region can have one member or multiple members with the same MST configuration; each member must be capable of processing RSTP bridge protocol data units (BPDUs). There is no limit to the number of MST regions in a network, but each region can support up to 65 spanning-tree instances. You can assign a VLAN to only one spanning-tree instance at a time.

IST, CIST, and CST

Unlike PVST+ and rapid PVST+ in which all the spanning-tree instances are independent, the MSTP establishes and maintains two types of spanning trees:

- An internal spanning tree (IST), which is the spanning tree that runs in an MST region.

  Within each MST region, the MSTP maintains multiple spanning-tree instances. Instance 0 is a special instance for a region, known as the internal spanning tree (IST). All other MST instances are numbered from 1 to 4094.

  The IST is the only spanning-tree instance that sends and receives BPDUs; all of the other spanning-tree instance information is contained in M-records, which are encapsulated within MSTP BPDUs. Because the MSTP BPDU carries information for all instances, the number of BPDUs that need to be processed by a switch to support multiple spanning-tree instances is significantly reduced.

  All MST instances within the same region share the same protocol timers, but each MST instance has its own topology parameters, such as root switch ID, root path cost, and so forth. By default, all VLANs are assigned to the IST.

  An MST instance is local to the region; for example, MST instance 1 in region A is independent of MST instance 1 in region B, even if regions A and B are interconnected.

- A common and internal spanning tree (CIST), which is a collection of the ISTs in each MST region, and the common spanning tree (CST) that interconnects the MST regions and single spanning trees.

  The spanning tree computed in a region appears as a subtree in the CST that encompasses the entire switched domain. The CIST is formed as a result of the spanning-tree algorithm running between switches that support the 802.1w, 802.1s, and 802.1D protocols. The CIST inside an MST region is the same as the CST outside a region.

For more information, see the "Operations Within an MST Region" section on page 12-3 and the "Operations Between MST Regions" section on page 12-4.

Note The implementation of the 802.1s standard changes some of the terminology associated with MST implementations. For a summary of these changes, see Table 12-1 on page 12-5.

Operations Within an MST Region

The IST connects all the MSTP switches in a region. When the IST converges, the root of the IST becomes the IST master (shown in Figure 12-1 on page 12-4), which is the switch within the region with the lowest bridge ID and path cost to the CST root. The IST master also is the CST root if there is only one region within the network. If the CST root is outside the region, one of the MSTP switches at the boundary of the region is selected as the IST master.

When an MSTP switch initializes, it sends BPDUs claiming itself as the root of the CST and the IST master, with both of the path costs to the CST root and to the IST master set to zero. The switch also initializes all of its MST instances and claims to be the root for all of them. If the switch receives superior MST root information (lower bridge ID, lower path cost, and so forth) than currently stored for the port, it relinquishes its claim as the IST master.

During initialization, a region might have many subregions, each with its own IST master. As switches receive superior IST information, they leave their old subregions and join the new subregion that might contain the true IST master. Thus all subregions shrink, except for the one that contains the true IST master.

For correct operation, all switches in the MST region must agree on the same IST master. Therefore, any two switches in the region synchronize their port roles for an MST instance only if they converge to a common IST master.

Operations Between MST Regions

If there are multiple regions or legacy 802.1D switches within the network, MSTP establishes and maintains the CST, which includes all MST regions and all legacy STP switches in the network. The MST instances combine with the IST at the boundary of the region to become the CST.

The IST connects all the MSTP switches in the region and appears as a subtree in the CST that encompasses the entire switched domain, with the root of the subtree being the IST master. The MST region appears as a virtual switch to adjacent STP switches and MST regions.

Figure 12-1 shows a network with three MST regions and a legacy 802.1D switch (D). The IST master for region 1 (A) is also the CST root. The IST master for region 2 (B) and the IST master for region 3 (C) are the roots for their respective subtrees within the CST. The RSTP runs in all regions.

Figure 12-1 MST Regions, IST Masters, and the CST Root

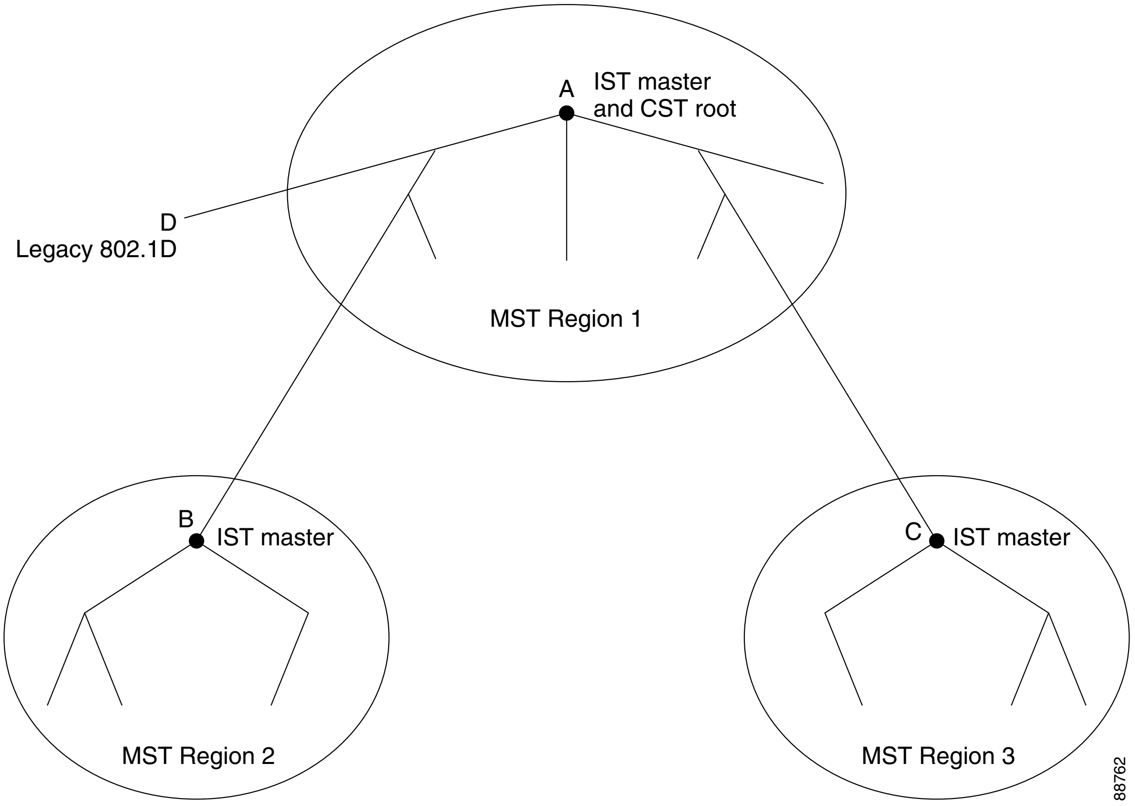


Figure 12-1 does not show additional MST instances for each region. Note that the topology of MST instances can be different from that of the IST for the same region.

Only the CST instance sends and receives BPDUs, and MST instances add their spanning-tree information into the BPDUs to interact with neighboring switches and compute the final spanning-tree topology. Because of this, the spanning-tree parameters related to BPDU transmission (for example, hello time, forward time, max-age, and max-hops) are configured only on the CST instance but affect all MST instances. Parameters related to the spanning-tree topology (for example, switch priority, port VLAN cost, port VLAN priority) can be configured on both the CST instance and the MST instance.

MSTP switches use Version 3 RSTP BPDUs or 802.1D STP BPDUs to communicate with legacy 802.1D switches. MSTP switches use MSTP BPDUs to communicate with MSTP switches.

IEEE 802.1s Terminology

Some MST naming conventions used in Cisco's prestandard implementation have been changed to identify some *internal* or *regional* parameters. These parameters are significant only within an MST region, as opposed to external parameters that are relevant to the whole network. Because the CIST is the only spanning-tree instance that spans the whole network, only the CIST parameters require the external rather than the internal or regional qualifiers.

- The CIST root is the root switch for the unique instance that spans the whole network, the CIST.
- The CIST external root path cost is the cost to the CIST root. This cost is left unchanged within an MST region. Remember that an MST region looks like a single switch for the CIST. The CIST external root path cost is the root path cost calculated between these virtual switches and switches that do not belong to any region.
- The CIST regional root was called the IST master in the prestandard implementation. If the CIST root is in the region, the CIST regional root is the CIST root. Otherwise, the CIST regional root is the closest switch to the CIST root in the region. The CIST regional root acts as a root switch for the IST.
- The CIST internal root path cost is the cost to the CIST regional root in a region. This cost is only relevant to the IST, instance 0.

Table 12-1 compares the IEEE standard and the Cisco prestandard terminology.

Table 12-1 Prestandard and Standard Terminology

IEEE Standard	Cisco Prestandard	Cisco Standard
CIST regional root	IST master	CIST regional root
CIST internal root path cost	IST master path cost	CIST internal path cost
CIST external root path cost	Root path cost	Root path cost
MSTI regional root	Instance root	Instance root
MSTI internal root path cost	Root path cost	Root path cost

Hop Count

The IST and MST instances do not use the message-age and maximum-age information in the configuration BPDU to compute the spanning-tree topology. Instead, they use the path cost to the root and a hop-count mechanism similar to the IP time-to-live (TTL) mechanism.

By using the **spanning-tree mst max-hops** global configuration command, you can configure the maximum hops inside the region and apply it to the IST and all MST instances in that region. The hop count achieves the same result as the message-age information (trigger a reconfiguration). The root switch of the instance always sends a BPDU (or M-record) with a cost of 0 and the hop count set to the maximum value. When a switch receives this BPDU, it decrements the received remaining hop count by one and propagates this value as the remaining hop count in the BPDUs it generates. When the count reaches zero, the switch discards the BPDU and ages the information held for the port.

The message-age and maximum-age information in the RSTP portion of the BPDU remain the same throughout the region, and the same values are propagated by the region's designated ports at the boundary.

Boundary Ports

In the Cisco prestandard implementation, a boundary port connects an MST region to a single spanning-tree region running RSTP, to a single spanning-tree region running PVST+ or rapid PVST+, or to another MST region with a different MST configuration. A boundary port also connects to a LAN, the designated switch of which is either a single spanning-tree switch or a switch with a different MST configuration.

Note On the Cisco Connected Grid switch, only NNIs or STP-enabled ENIs can be MST ports. UNIs do not participate in STP.

There is no definition of a boundary port in the 802.1s standard. The 802.1Q-2002 standard identifies two kinds of messages that a port can receive: internal (coming from the same region) and external. When a message is external, it is received only by the CIST. If the CIST role is root or alternate, or if the external BPDU is a topology change, it could have an impact on the MST instances. When a message is internal, the CIST part is received by the CIST, and each MST instance receives its respective M-record. The Cisco prestandard implementation treats a port that receives an external message as a boundary port. This means a port cannot receive a mix of internal and external messages.

An MST region includes both switches and LANs. A segment belongs to the region of its designated port. Therefore, a port in a different region than the designated port for a segment is a boundary port. This definition allows two ports internal to a region to share a segment with a port belonging to a different region, creating the possibility of receiving both internal and external messages on a port.

The primary change from the Cisco prestandard implementation is that a designated port is not defined as boundary, unless it is running in an STP-compatible mode.

Note If there is a legacy STP switch on the segment, messages are always considered external.

The other change from the prestandard implementation is that the CIST regional root switch ID field is now inserted where an RSTP or legacy 802.1Q switch has the sender switch ID. The whole region performs like a single virtual switch by sending a consistent sender switch ID to neighboring switches. In the example in Figure 12-1, switch C would receive a BPDU with the same consistent sender switch ID of root, whether or not A or B is designated for the segment.

IEEE 802.1s Implementation

The Cisco implementation of the IEEE MST standard includes features required to meet the standard, as well as some of the desirable prestandard functionality that is not yet incorporated into the published standard.

Port Role Naming Change

The boundary role is no longer in the final MST standard, but this boundary concept is maintained in Cisco's implementation. However, an MST instance port at a boundary of the region might not follow the state of the corresponding CIST port. Two cases exist now:

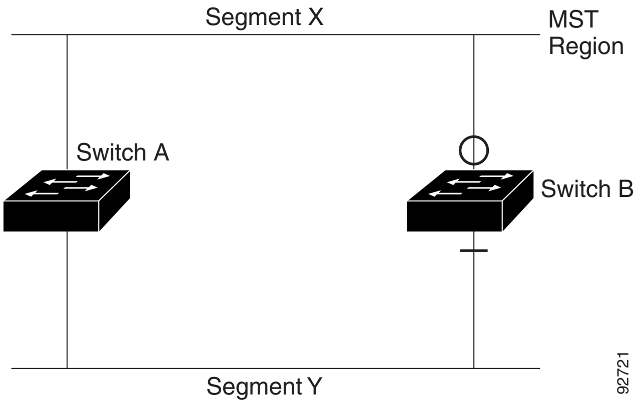
- The boundary port is the root port of the CIST regional root—When the CIST instance port is proposed and is in sync, it can send back an agreement and move to the forwarding state only after all the corresponding MSTI ports are in sync (and thus forwarding). The MSTI ports now have a special *master* role.
- The boundary port is not the root port of the CIST regional root—The MSTI ports follow the state and role of the CIST port. The standard provides less information, and it might be difficult to understand why an MSTI port can be alternately blocking when it receives no BPDUs (MRecords). In this case, although the boundary role no longer exists, the **show** commands identify a port as boundary in the *type* column of the output.

Interoperation Between Legacy and Standard Switches

Because automatic detection of prestandard switches can fail, you can use an interface configuration command to identify prestandard ports. A region cannot be formed between a standard and a prestandard switch, but they can interoperate by using the CIST. Only the capability of load balancing over different instances is lost in that particular case. The CLI displays different flags depending on the port configuration when a port receives prestandard BPDUs. A syslog message also appears the first time a switch receives a prestandard BPDU on a port that has not been configured for prestandard BPDU transmission.

Figure 12-2 illustrates this scenario. Assume that A is a standard switch and B a prestandard switch, both configured to be in the same region. A is the root switch for the CIST, and thus B has a root port (BX) on segment X and an alternate port (BY) on segment Y. If segment Y flaps, and the port on BY becomes the alternate before sending out a single prestandard BPDU, AY cannot detect that a prestandard switch is connected to Y and continues to send standard BPDUs. The port BY is thus fixed in a boundary, and no load balancing is possible between A and B. The same problem exists on segment X, but B might transmit topology changes.

Figure 12-2 Standard and Prestandard Switch Interoperation



Note We recommend that you minimize the interaction between standard and prestandard MST implementations.

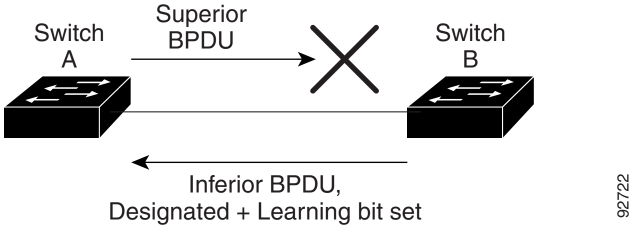
Detecting Unidirectional Link Failure

This feature is not yet present in the IEEE MST standard, but it is included in this Cisco IOS release. The software checks the consistency of the port role and state in the received BPDUs to detect unidirectional link failures that could cause bridging loops.

When a designated port detects a conflict, it keeps its role, but reverts to discarding state because disrupting connectivity in case of inconsistency is preferable to opening a bridging loop.

Figure 12-3 illustrates a unidirectional link failure that typically creates a bridging loop. Switch A is the root switch, and its BPDUs are lost on the link leading to switch B. RSTP and MST BPDUs include the role and state of the sending port. With this information, switch A can detect that switch B does not react to the superior BPDUs it sends and that switch B is the designated, not root switch. As a result, switch A blocks (or keeps blocking) its port, thus preventing the bridging loop.

Figure 12-3 Detecting Unidirectional Link Failure



Interoperability with IEEE 802.1D STP

A switch running MSTP supports a built-in protocol migration mechanism that enables it to interoperate with legacy 802.1D switches. If this switch receives a legacy 802.1D configuration BPDU (a BPDU with the protocol version set to 0), it sends only 802.1D BPDUs on that port. An MSTP switch also can detect that a port is at the boundary of a region when it receives a legacy BPDU, an MSTP BPDU (Version 3) associated with a different region, or an RSTP BPDU (Version 2).

However, the switch does not automatically revert to the MSTP mode if it no longer receives 802.1D BPDUs because it cannot detect whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. Also, a switch might continue to assign a boundary role to a port when the switch to which this switch is connected has joined the region. To restart the protocol migration process (force the renegotiation with neighboring switches), use the **clear spanning-tree detected-protocols** privileged EXEC command.

If all the legacy switches on the link are RSTP switches, they can process MSTP BPDUs as if they are RSTP BPDUs. Therefore, MSTP switches send either a Version 0 configuration and TCN BPDUs or Version 3 MSTP BPDUs on a boundary port. A boundary port connects to a LAN, the designated switch of which is either a single spanning-tree switch or a switch with a different MST configuration.

Information About RSTP

The RSTP takes advantage of point-to-point wiring and provides rapid convergence of the spanning tree. Reconfiguration of the spanning tree can occur in less than 1 second (in contrast to 50 seconds with the default settings in the 802.1D spanning tree), which is critical for networks carrying delay-sensitive traffic such as voice and video.

- Port Roles and the Active Topology, page 12-9
- Rapid Convergence, page 12-10
- Synchronization of Port Roles, page 12-11
- Bridge Protocol Data Unit Format and Processing, page 12-12

For configuration information, see the "Guidelines and Limitations" section on page 12-14.

Port Roles and the Active Topology

The RSTP provides rapid convergence of the spanning tree by assigning port roles and by learning the active topology. The RSTP builds upon the 802.1D STP to select the switch with the highest switch priority (lowest numerical priority value) as the root switch as described in Spanning-Tree Topology and BPDUs, page 11-3. Then the RSTP assigns one of these port roles to individual ports.

Note On the Cisco Connected Grid switch, only NNIs or STP-enabled ENIs can be RSTP ports. UNIs do not participate in STP.

- Root port—Provides the best path (lowest cost) when the switch forwards packets to the root switch.
- Designated port—Connects to the designated switch, which incurs the lowest path cost when forwarding packets from that LAN to the root switch. The port through which the designated switch is attached to the LAN is called the designated port.
- Alternate port—Offers an alternate path toward the root switch to that provided by the current root port.
- Backup port—Acts as a backup for the path provided by a designated port toward the leaves of the spanning tree. A backup port can exist only when two ports are connected together in a loopback by a point-to-point link or when a switch has two or more connections to a shared LAN segment.
- Disabled port—Has no role within the operation of the spanning tree.

A port with the root or a designated port role is included in the active topology. A port with the alternate or backup port role is excluded from the active topology.

In a stable topology with consistent port roles throughout the network, the RSTP ensures that every root port and designated port immediately transition to the forwarding state while all alternate and backup ports are always in the discarding state (equivalent to blocking in 802.1D). The port state controls the operation of the forwarding and learning processes. Table 12-2 provides a comparison of 802.1D and RSTP port states.

Table 12-2 Port State Comparison

Operational Status	STP Port State (802.1D)	RSTP Port State	Is Port Included in the Active Topology?
Enabled	Blocking	Discarding	No
Enabled	Listening	Discarding	No
Enabled	Learning	Learning	Yes
Enabled	Forwarding	Forwarding	Yes
Disabled	Disabled	Discarding	No

To be consistent with Cisco STP implementations, this guide documents the port state as *blocking* instead of *discarding*. Designated ports start in the listening state.

Rapid Convergence

The RSTP provides for rapid recovery of connectivity following the failure of a switch, a switch port, or a LAN. It provides rapid convergence for edge ports, new root ports, and ports connected through point-to-point links as follows:

- Edge ports—If you configure a port as an edge port on an RSTP switch by using the **spanning-tree portfast** interface configuration command, the edge port immediately transitions to the forwarding state. An edge port is the same as a Port Fast-enabled port, and you should enable it only on ports that connect to a single end station.
- Root ports—If the RSTP selects a new root port, it blocks the old root port and immediately transitions the new root port to the forwarding state.
- Point-to-point links—If you connect a port to another port through a point-to-point link and the local port becomes a designated port, it negotiates a rapid transition with the other port by using the proposal-agreement handshake to ensure a loop-free topology.

Note On the Cisco Connected Grid switch, these ports are always NNIs or STP-enabled ENIs.

As shown in Figure 12-4, Switch A is connected to Switch B through a point-to-point link, and all of the ports are in the blocking state. Assume that the priority of Switch A is a smaller numerical value than the priority of Switch B. Switch A sends a proposal message (a configuration BPDU with the proposal flag set) to Switch B, proposing itself as the designated switch.

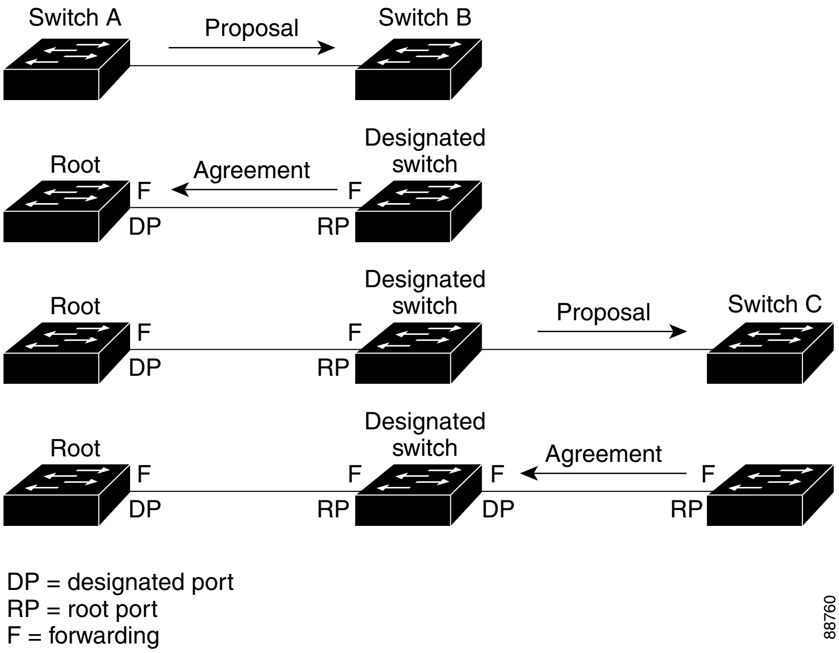
After receiving the proposal message, Switch B selects as its new root port the port from which the proposal message was received, forces all nonedge ports to the blocking state, and sends an agreement message (a BPDU with the agreement flag set) through its new root port.

After receiving Switch B's agreement message, Switch A also immediately transitions its designated port to the forwarding state. No loops in the network are formed because Switch B blocked all of its nonedge ports and because there is a point-to-point link between Switches A and B.

When Switch C is connected to Switch B, a similar set of handshaking messages are exchanged. Switch C selects the port connected to Switch B as its root port, and both ends immediately transition to the forwarding state. With each iteration of this handshaking process, one more switch joins the active topology. As the network converges, this proposal-agreement handshaking progresses from the root toward the leaves of the spanning tree.

The switch learns the link type from the port duplex mode: a full-duplex port is considered to have a point-to-point connection; a half-duplex port is considered to have a shared connection. You can override the default setting that is controlled by the duplex setting by using the **spanning-tree link-type** interface configuration command.

Figure 12-4 Proposal and Agreement Handshaking for Rapid Convergence



Synchronization of Port Roles

When the switch receives a proposal message on one of its ports and that port is selected as the new root port, the RSTP forces all other ports to synchronize with the new root information.

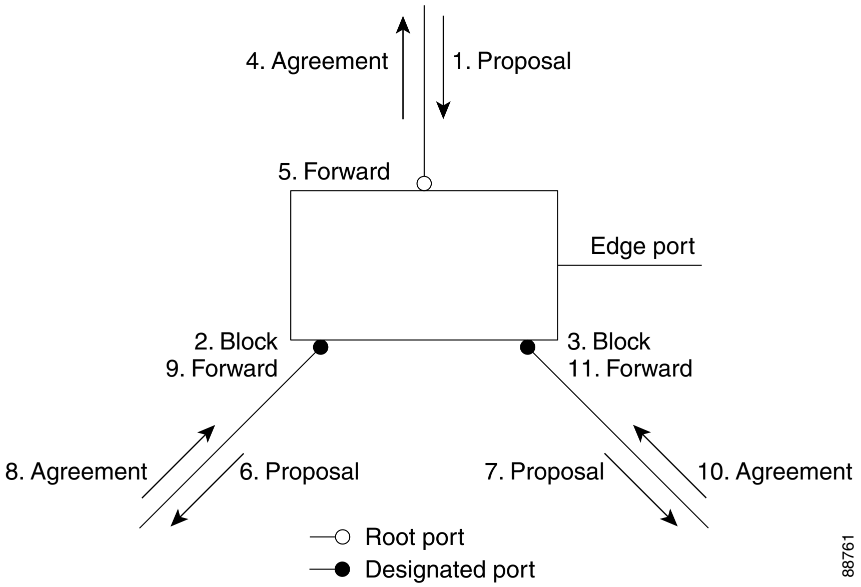
The switch is synchronized with superior root information received on the root port if all other ports are synchronized. An individual port on the switch is synchronized if

- That port is in the blocking state.
- It is an edge port (a port configured to be at the edge of the network).

If a designated STP port is in the forwarding state and is not configured as an edge port, it transitions to the blocking state when the RSTP forces it to synchronize with new root information. In general, when the RSTP forces a port to synchronize with root information and the port does not satisfy any of the above conditions, its port state is set to blocking.

After ensuring all of the ports are synchronized, the switch sends an agreement message to the designated switch corresponding to its root port. When the switches connected by a point-to-point link are in agreement about their port roles, the RSTP immediately transitions the port states to forwarding. The sequence of events is shown in Figure 12-5.

Figure 12-5 Sequence of Events During Rapid Convergence



Bridge Protocol Data Unit Format and Processing

The RSTP BPDU format is the same as the 802.1D BPDU format except that the protocol version is set to 2. A new one-byte Version 1 Length field is set to zero, which means that no version 1 protocol information is present. Table 12-3 shows the RSTP flag fields.

Table 12-3 RSTP BPDU Flags

Bit	Function
0	Topology change (TC)
1	Proposal
2–3:	Port role:
00	Unknown
01	Alternate port
10	Root port
11	Designated port
4	Learning
5	Forwarding
6	Agreement
7	Topology change acknowledgement (TCA)

The sending switch sets the proposal flag in the RSTP BPDU to propose itself as the designated switch on that LAN. The port role in the proposal message is always set to the designated port.

The sending switch sets the agreement flag in the RSTP BPDU to accept the previous proposal. The port role in the agreement message is always set to the root port.

The RSTP does not have a separate topology change notification (TCN) BPDU. It uses the topology change (TC) flag to show the topology changes. However, for interoperability with 802.1D switches, the RSTP switch processes and generates TCN BPDUs.

The learning and forwarding flags are set according to the state of the sending port.

Processing Superior BPDU Information

If a port receives superior root information (lower bridge ID, lower path cost, and so forth) than currently stored for the port, the RSTP triggers a reconfiguration. If the port is proposed and is selected as the new root port, RSTP forces all the other ports to synchronize.

If the BPDU received is an RSTP BPDU with the proposal flag set, the switch sends an agreement message after all of the other ports are synchronized. If the BPDU is an 802.1D BPDU, the switch does not set the proposal flag and starts the forward-delay timer for the port. The new root port requires twice the forward-delay time to transition to the forwarding state.

If the superior information received on the port causes the port to become a backup or alternate port, RSTP sets the port to the blocking state but does not send the agreement message. The designated port continues sending BPDUs with the proposal flag set until the forward-delay timer expires, at which time the port transitions to the forwarding state.

Processing Inferior BPDU Information

If a designated port receives an inferior BPDU (higher bridge ID, higher path cost, and so forth than currently stored for the port) with a designated port role, it immediately replies with its own information.

Topology Changes

This section describes the differences between the RSTP and the 802.1D in handling spanning-tree topology changes.

- Detection—Unlike 802.1D in which *any* transition between the blocking and the forwarding state causes a topology change, *only* transitions from the blocking to the forwarding state cause a topology change with RSTP (only an increase in connectivity is considered a topology change). State changes on an edge port do not cause a topology change. When an RSTP switch detects a topology change, it flushes the learned information on all of its nonedge ports except on those from which it received the TC notification.
- Notification—Unlike 802.1D, which uses TCN BPDUs, the RSTP does not use them. However, for 802.1D interoperability, an RSTP switch processes and generates TCN BPDUs.
- Acknowledgement—When an RSTP switch receives a TCN message on a designated port from an 802.1D switch, it replies with an 802.1D configuration BPDU with the TCA bit set. However, if the TC-while timer (the same as the topology-change timer in 802.1D) is active on a root port connected to an 802.1D switch and a configuration BPDU with the TCA bit set is received, the TC-while timer is reset.

  This behavior is only required to support 802.1D switches. The RSTP BPDUs never have the TCA bit set.
- Propagation—When an RSTP switch receives a TC message from another switch through a designated or root port, it propagates the change to all of its nonedge, designated ports and to the root port (excluding the port on which it is received). The switch starts the TC-while timer for all such ports and flushes the information learned on them.

- Protocol migration—For backward compatibility with 802.1D switches, RSTP selectively sends 802.1D configuration BPDUs and TCN BPDUs on a per-port basis.

  When a port is initialized, the migrate-delay timer is started (specifies the minimum time during which RSTP BPDUs are sent), and RSTP BPDUs are sent. While this timer is active, the switch processes all BPDUs received on that port and ignores the protocol type.

  If the switch receives an 802.1D BPDU after the port's migration-delay timer has expired, it assumes that it is connected to an 802.1D switch and starts using only 802.1D BPDUs. However, if the RSTP switch is using 802.1D BPDUs on a port and receives an RSTP BPDU after the timer has expired, it restarts the timer and starts using RSTP BPDUs on that port.

Prerequisites

- Be familiar with the information in the "Information About MSTP" section on page 12-2, "Information About RSTP" section on page 12-8, and "Guidelines and Limitations" section on page 12-14.
- Ensure that your network strategy and planning for your network are complete.
- Ensure that STP is enabled.

Guidelines and Limitations

- On the Cisco Connected Grid switch, MSTP is supported only on NNIs or ENIs on which STP has been enabled. You enable STP on an ENI by entering the **spanning-tree** interface configuration command. UNIs do not participate in MSTP.
- When you enable MST by using the **spanning-tree mode mst** global configuration command, RSTP is automatically enabled.
- For two or more switches to be in the same MST region, they must have the same VLAN-to-instance map, the same configuration revision number, and the same name.
- The switch supports up to 65 MST instances. The number of VLANs that can be mapped to a particular MST instance is unlimited.
- PVST+, rapid PVST+, and MSTP are supported, but only one version can be active at any time. (For example, all VLANs run PVST+, all VLANs run rapid PVST+, or all VLANs run MSTP.) For more information, see the "Spanning-Tree Interoperability and Backward Compatibility" section on page 11-10. For information on the recommended trunk port configuration, see the "Interaction with Other Features" section on page 4-3.
- You can manually configure the MST configuration (region name, revision number, and VLAN-to-instance mapping) on each switch within the MST region by using the command-line interface (CLI) or through the SNMP support.
- For load balancing across redundant paths in the network to work, all VLAN-to-instance mapping assignments must match; otherwise, all traffic flows on a single link.
- All MST boundary ports must be forwarding for load balancing between a PVST+ and an MST cloud or between a rapid-PVST+ and an MST cloud. For this to occur, the IST master of the MST cloud should also be the root of the CST. If the MST cloud consists of multiple MST regions, one of the MST regions must contain the CST root, and all of the other MST regions must have a better path to the root contained within the MST cloud than a path through the PVST+ or rapid-PVST+ cloud. You might have to manually configure the switches in the clouds.

- Partitioning the network into a large number of regions is not recommended. However, if this situation is unavoidable, we recommend that you partition the switched LAN into smaller LANs interconnected by routers or non-Layer 2 devices.

Default Settings

Feature	Default Setting
Spanning-tree mode	Rapid PVST+ (PVST+ and MSTP are disabled).
Switch priority (configurable on a per-CIST port basis)	32768.
Spanning-tree port priority (configurable on a per-CIST port basis)	128.
Spanning-tree port cost (configurable on a per-CIST port basis)	1000 Mbps: 4. 100 Mbps: 19. 10 Mbps: 100.
Hello time	2 seconds.
Forward-delay time	15 seconds.
Maximum-aging time	20 seconds.
Maximum hop count	20 hops.

For information about the supported number of spanning-tree instances, see the "Supported Spanning-Tree Instances" section on page 11-10.

Configuring MSTP Features

This section includes the following topics:

- Specifying the MST Region Configuration and Enabling MSTP, page 12-16 (required)
- Configuring the Root Switch, page 12-17 (optional)
- Configuring a Secondary Root Switch, page 12-19 (optional)
- Configuring Port Priority, page 12-21 (optional)
- Configuring Path Cost, page 12-22 (optional)
- Configuring the Switch Priority, page 12-24 (optional)
- Configuring the Hello Time, page 12-25 (optional)
- Configuring the Forwarding-Delay Time, page 12-26 (optional)
- Configuring the Maximum-Aging Time, page 12-26 (optional)
- Configuring the Maximum-Hop Count, page 12-27 (optional)
- Specifying the Link Type to Ensure Rapid Transitions, page 12-28 (optional)
- Designating the Neighbor Type, page 12-29 (optional)

- Restarting the Protocol Migration Process, page 12-30 (optional)

Specifying the MST Region Configuration and Enabling MSTP

Follow this procedure to configure the MST region and enable MSTP. This procedure is required.

BEFORE YOU BEGIN

- For two or more switches to be in the same MST region, they must have the same VLAN-to-instance mapping, the same configuration revision number, and the same name.
- A region can have one member or multiple members with the same MST configuration; each member must be capable of processing RSTP BPDUs. There is no limit to the number of MST regions in a network, but each region can support up to 65 spanning-tree instances. You can assign a VLAN to only one spanning-tree instance at a time.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree mst configuration**	Enter MST configuration mode.
Step 3	**instance** *instance-id* **vlan** *vlan-range*	Map VLANs to an MST instance. • For *instance-id*, the range is 0 to 4094. • For **vlan** *vlan-range*, the range is 1 to 4094. When you map VLANs to an MST instance, the mapping is incremental, and the VLANs specified in the command are added to or removed from the VLANs that were previously mapped. To specify a VLAN range, use a hyphen; for example, **instance 1 vlan 1-63** maps VLANs 1 through 63 to MST instance 1. To specify a VLAN series, use a comma; for example, **instance 1 vlan 10, 20, 30** maps VLANs 10, 20, and 30 to MST instance 1.
Step 4	**name** *name*	Specify the configuration name. The *name* string has a maximum length of 32 characters and is case sensitive.
Step 5	**revision** *version*	Specify the configuration revision number. The range is 0 to 65535.
Step 6	**show pending**	Verify your configuration by displaying the pending configuration.
Step 7	**exit**	Apply all changes, and return to global configuration mode.

	Command	Purpose
Step 8	**spanning-tree mode mst**	Enable MSTP. RSTP is also enabled. **Caution** Changing spanning-tree modes can disrupt traffic because all spanning-tree instances are stopped for the previous mode and restarted in the new mode. You cannot run both MSTP and rapid PVST+ or both MSTP and PVST+ at the same time.
Step 9	**end**	Return to privileged EXEC mode.
Step 10	**show running-config**	Verify your entries.
Step 11	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default MST region configuration, use the **no spanning-tree mst configuration** global configuration command. To return to the default VLAN-to-instance map, use the **no instance** *instance-id* [**vlan** *vlan-range*] MST configuration command. To return to the default name, use the **no name** MST configuration command. To return to the default revision number, use the **no revision** MST configuration command. To re-enable rapid PVST+, use the **no spanning-tree mode** or the **spanning-tree mode pvst** global configuration command.

EXAMPLE

This example shows how to enter MST configuration mode, map VLANs 10 to 20 to MST instance 1, name the region *region1*, set the configuration revision to 1, display the pending configuration, apply the changes, and return to global configuration mode:

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
--------  ---------------------
0         1-9,21-4094
1         10-20
-------------------------------

Switch(config-mst)# exit
Switch(config)#
```

Configuring the Root Switch

The switch maintains a spanning-tree instance for the group of VLANs mapped to it. A bridge ID, consisting of the switch priority and the switch MAC address, is associated with each instance. For a group of VLANs, the switch with the lowest bridge ID becomes the root switch.

To configure a switch to become the root, use the **spanning-tree mst** *instance-id* **root** global configuration command to modify the switch priority from the default value (32768) to a significantly lower value so that the switch becomes the root switch for the specified spanning-tree instance. When you enter this command, the switch checks the switch priorities of the root switches. Because of the extended system ID support, the switch sets its own priority for the specified instance to 24576 if this value will cause this switch to become the root for the specified spanning-tree instance.

If any root switch for the specified instance has a switch priority lower than 24576, the switch sets its own priority to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value as shown in Table 11-1.)

If your network consists of switches that both do and do not support the extended system ID, it is unlikely that the switch with the extended system ID support will become the root switch. The extended system ID increases the switch priority value every time the VLAN number is greater than the priority of the connected switches running older software.

Note After configuring the switch as the root switch, we recommend that you avoid manually configuring the hello time, forward-delay time, and maximum-age time through the **spanning-tree mst hello-time**, **spanning-tree mst forward-time**, and the **spanning-tree mst max-age** global configuration commands.

Follow this procedure to configure a switch as the root switch. This procedure is optional.

BEFORE YOU BEGIN

- The root switch for each spanning-tree instance should be a backbone or distribution switch. Do not configure an access switch as the spanning-tree primary root.
- Use the **diameter** keyword, which is available only for MST instance 0, to specify the Layer 2 network diameter (that is, the maximum number of switch hops between any two end stations in the Layer 2 network). When you specify the network diameter, the switch automatically sets an optimal hello time, forward-delay time, and maximum-age time for a network of that diameter, which can significantly reduce the convergence time. You can use the **hello** keyword to override the automatically calculated hello time.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree mst** *instance-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	Configure a switch as the root switch. • For *instance-id*, you can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094. • (Optional) For **diameter** *net-diameter*, specify the maximum number of switches between any two end stations. The range is 2 to 7. This keyword is available only for MST instance 0. • (Optional) For **hello-time** *seconds*, specify the interval in seconds between the generation of configuration messages by the root switch. The range is 1 to 10 seconds; the default is 2 seconds.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree mst** *instance-id*	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no spanning-tree mst** *instance-id* **root** global configuration command.

EXAMPLE

This example configures MST instance 0 as the root switch:

```
Switch(config)# spanning-tree mst 0 root primary
    mst 0 bridge priority set to 24576
    mst bridge max aging time unchanged at 20
    mst bridge hello time unchanged at 2
    mst bridge forward delay unchanged at 15
Switch(config)# end
Switch#
```

Configuring a Secondary Root Switch

When you configure a switch with the extended system ID support as the secondary root, the switch priority is modified from the default value (32768) to 28672. The switch is then likely to become the root switch for the specified instance if the primary root switch fails. This is assuming that the other network switches use the default switch priority of 32768 and therefore are unlikely to become the root switch.

Follow this procedure to configure a switch as the secondary root switch. This procedure is optional.

BEFORE YOU BEGIN

- Configure the root switch as described in the "Configuring the Root Switch" procedure on page 12-17.

- You can execute this command on more than one switch to configure multiple backup root switches. Use the same network diameter and hello-time values that you used when you configured the primary root switch with the **spanning-tree mst** *instance-id* **root primary** global configuration command.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree mst** *instance-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	Configure a switch as the secondary root switch. • For *instance-id*, you can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094. • (Optional) For **diameter** *net-diameter*, specify the maximum number of switches between any two end stations. The range is 2 to 7. This keyword is available only for MST instance 0. • (Optional) For **hello-time** *seconds*, specify the interval in seconds between the generation of configuration messages by the root switch. The range is 1 to 10 seconds; the default is 2 seconds. Use the same network diameter and hello-time values that you used when configuring the primary root switch. See the "Configuring the Root Switch" section on page 12-17.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree mst** *instance-id*	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no spanning-tree mst** *instance-id* **root** global configuration command.

EXAMPLE

This example configures MST instance 5 as the secondary root switch:

```
Switch(config)# spanning-tree mst 5 root secondary
    mst 5 bridge priority set to 16384
    mst bridge max aging time unchanged at 20
    mst bridge hello time unchanged at 2
    mst bridge forward delay unchanged at 15
Switch(config)# end
Switch#
```

Configuring Port Priority

If a loop occurs, the MSTP uses the port priority when selecting an STP port to put into the forwarding state. You can assign higher priority values (lower numerical values) to STP ports that you want selected first and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, the MSTP puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

Follow this procedure to configure the MSTP port priority of an interface. This procedure is optional.

BEFORE YOU BEGIN

- If a physical interface is a UNI, before attempting to configure MST port priority, you must enter the **port-type nni** interface configuration command or configure the port as an ENI and enable spanning tree on the port. (See the "Enabling Spanning Tree on an ENI" section on page 11-13.)
- If the interface is a VLAN, only ports with spanning tree enabled in the VLAN will run spanning tree.
- If the interface is a port channel, all members of the port channel must be NNIs or ENIs with spanning tree enabled.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify an interface to configure, and enter interface configuration mode. Valid interfaces include physical NNIs or ENIs with spanning tree enabled, VLANs, and NNI or ENI port channels. The VLAN ID range is 1 to 4094. The port-channel range is 1 to 48.
Step 3	**spanning-tree mst** *instance-id* **port-priority** *priority*	Configure the port priority. • For *instance-id*, you can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094. • For *priority*, the range is 0 to 240 in increments of 16. The default is 128. The lower the number, the higher the priority. The priority values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected.
Step 4	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 5	**show spanning-tree mst interface** *interface-id* or **show spanning-tree mst** *instance-id*	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note The **show spanning-tree mst interface** *interface-id* privileged EXEC command displays information only if the port is in a link-up operative state. Otherwise, you can use the **show running-config interface** privileged EXEC command to confirm the configuration.

To return the interface to its default setting, use the **no spanning-tree mst** *instance-id* **port-priority** interface configuration command.

EXAMPLE

The following example shows how to increase the likelihood that spanning-tree instance 20 is chosen as the root-bridge on interface Ethernet 2/0:

```
Switch(config)# interface ethernet 2/0
Switch(config-if)# spanning-tree port-priority 20
Switch(config-if)#
```

Configuring Path Cost

The MSTP path cost default value is derived from the media speed of an STP port. If a loop occurs, the MSTP uses cost when selecting an interface to put in the forwarding state. You can assign lower cost values to STP ports that you want selected first and higher cost values that you want selected last. If all interfaces have the same cost value, the MSTP puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

Follow this procedure to configure the MSTP cost of an interface. This procedure is optional.

BEFORE YOU BEGIN

- If a physical interface is a UNI, before attempting to configure MST path cost, you must enter the **port-type nni** interface configuration command or configure the port as an ENI and enable spanning tree on the port. (See the "Enabling Spanning Tree on an ENI" section on page 11-13.)
- If the interface is a VLAN, only ports with spanning tree enabled in the VLAN will run spanning tree.
- If the interface is a port channel, all members of the port channel must be NNIs or ENIs with spanning tree enabled.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify an interface to configure, and enter interface configuration mode. Valid interfaces include physical NNIs or ENIs with spanning tree enabled, VLANs, and NNI or ENI port channels. The VLAN ID range is 1 to 4094. The port-channel range is 1 to 48.
Step 3	**spanning-tree mst** *instance-id* **cost** *cost*	Configure the cost. If a loop occurs, the MSTP uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission. • For *instance-id*, you can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094. • For *cost*, the range is 1 to 200000000; the default value is derived from the media speed of the interface.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show spanning-tree mst interface** *interface-id* or **show spanning-tree mst** *instance-id*	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note The **show spanning-tree mst interface** *interface-id* privileged EXEC command displays information only for ports that are in a link-up operative state. Otherwise, you can use the **show running-config** privileged EXEC command to confirm the configuration.

To return the interface to its default setting, use the **no spanning-tree mst** *instance-id* **cost** interface configuration command.

EXAMPLE

This example shows how to set the interface path cost:

```
Switch(config)# interface fastethernet 4/4
Switch(config-if)# spanning-tree mst 0 cost 17031970
Switch(config-if)# end
```

Configuring the Switch Priority

You can configure the switch priority and make it more likely that the switch will be chosen as the root switch. This procedure is optional.

BEFORE YOU BEGIN

Exercise care when using this command. For most situations, we recommend that you use the **spanning-tree mst** *instance-id* **root primary** and the **spanning-tree mst** *instance-id* **root secondary** global configuration commands to modify the switch priority.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree mst** *instance-id* **priority** *priority*	Configure the switch priority. • For *instance-id*, you can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094. • For *priority*, the range is 0 to 61440 in increments of 4096; the default is 32768. The lower the number, the more likely the switch will be chosen as the root switch. Priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree mst** *instance-id*	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no spanning-tree mst** *instance-id* **priority** global configuration command.

EXAMPLE

This example shows how to set the switch priority:

```
Switch(config)# spanning-tree mst 0 priority 4096
Switch(config)# end
```

Configuring the Hello Time

You can configure the interval between the generation of configuration messages by the root switch by changing the hello time. This procedure is optional.

BEFORE YOU BEGIN

Exercise care when using this command. For most situations, we recommend that you use the **spanning-tree mst** *instance-id* **root primary** and the **spanning-tree mst** *instance-id* **root secondary** global configuration commands to modify the hello time.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree mst hello-time** *seconds*	Configure the hello time for all MST instances. The hello time is the interval between the generation of configuration messages by the root switch. These messages mean that the switch is alive. For *seconds*, the range is 1 to 10; the default is 2.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree mst**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no spanning-tree mst hello-time** global configuration command.

EXAMPLE

This example shows how to set the hello-time delay timer:

```
Switch(config)# spanning-tree mst hello-time 3
Switch(config)# end
```

Configuring the Forwarding-Delay Time

Follow this procedure to configure the forwarding-delay time for all MST instances. This procedure is optional.

BEFORE YOU BEGIN

Exercise care when using this command. For most situations, we recommend that you use the **spanning-tree mst** *instance-id* **root primary** and the **spanning-tree mst** *instance-id* **root secondary** global configuration commands to modify the forwarding-delay time.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree mst forward-time** *seconds*	Configure the forward time for all MST instances. The forward delay is the number of seconds a port waits before changing from its spanning-tree learning and listening states to the forwarding state. For *seconds*, the range is 4 to 30; the default is 15.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree mst**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no spanning-tree mst forward-time** global configuration command.

EXAMPLE

This example shows how to set the forward-delay timer:

```
Switch(config)# spanning-tree mst forward-time 20
Switch(config)# end
```

Configuring the Maximum-Aging Time

Follow this procedure to configure the maximum-aging time for all MST instances. This procedure is optional.

BEFORE YOU BEGIN

Exercise care when using this command. For most situations, we recommend that you use the **spanning-tree mst** *instance-id* **root primary** and the **spanning-tree mst** *instance-id* **root secondary** global configuration commands to modify the maximum-aging time.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree mst max-age** *seconds*	Configure the maximum-aging time for all MST instances. The maximum-aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration. For *seconds*, the range is 6 to 40; the default is 20.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree mst**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no spanning-tree mst max-age** global configuration command.

EXAMPLE

This example shows how to set the max-age timer:

```
Switch(config)# spanning-tree mst max-age 40
Switch(config)# end
```

Configuring the Maximum-Hop Count

Follow this procedure to configure the maximum-hop count for all MST instances. This procedure is optional.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree mst max-hops** *hop-count*	Specify the number of hops in a region before the BPDU is discarded, and the information held for a port is aged. For *hop-count*, the range is 1 to 255; the default is 20.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree mst**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no spanning-tree mst max-hops** global configuration command.

EXAMPLE

This example shows how to set the number of possible hops:

```
Switch(config)# spanning-tree mst max-hops 25
Switch(config)# end
```

Specifying the Link Type to Ensure Rapid Transitions

If you connect an STP port to another STP port through a point-to-point link and the local port becomes a designated port, the RSTP negotiates a rapid transition with the other port by using the proposal-agreement handshake to ensure a loop-free topology as described in the "Rapid Convergence" section on page 12-10.

By default, the link type is controlled from the duplex mode of the interface: a full-duplex port is considered to have a point-to-point connection; a half-duplex port is considered to have a shared connection. If you have a half-duplex link physically connected point-to-point to a single port on a remote switch running MSTP, you can override the default setting of the link type and enable rapid transitions to the forwarding state. This procedure is optional.

BEFORE YOU BEGIN

- If a physical interface is a UNI, before attempting to configure the MST link type, you must enter the **port-type nni** interface configuration command or configure the port as an ENI and enable spanning tree on the port. (See the "Enabling Spanning Tree on an ENI" section on page 11-13.)
- If the interface is a VLAN, only ports with spanning tree enabled in the VLAN will run spanning tree.
- If the interface is a port channel, all members of the port channel must be NNIs or ENIs with spanning tree enabled.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify an interface to configure, and enter interface configuration mode. Valid interfaces include physical NNIs or ENIs with spanning tree enabled, VLANs, and NNI or ENI port channels. The VLAN ID range is 1 to 4094. The port-channel range is 1 to 48.
Step 3	**spanning-tree link-type point-to-point**	Specify that the link type of a port is point-to-point.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show spanning-tree mst interface** *interface-id*	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the port to its default setting, use the **no spanning-tree link-type** interface configuration command.

EXAMPLE

This example shows how to configure the port as a point-to-point link:

```
Switch(config-if)# spanning-tree link-type point-to-point
Switch(config-if)# end
```

Designating the Neighbor Type

A topology could contain both prestandard and 802.1s standard compliant devices. By default, ports can automatically detect prestandard devices, but they can still receive both standard and prestandard BPDUs. When there is a mismatch between a device and its neighbor, only the CIST runs on the interface.

You can choose to set a port to send only prestandard BPDUs. The prestandard flag appears in all the **show** commands, even if the port is in STP compatibility mode. This procedure is optional.

BEFORE YOU BEGIN

- If a physical interface is a UNI, before attempting to configure the neighbor type, you must enter the **port-type nni** interface configuration command or configure the port as an ENI and enable spanning tree on the port. (See the "Enabling Spanning Tree on an ENI" section on page 11-13.)
- If the interface is a VLAN, only ports with spanning tree enabled in the VLAN will run spanning tree.
- If the interface is a port channel, all members of the port channel must be NNIs or ENIs with spanning tree enabled.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify an interface to configure, and enter interface configuration mode. Valid interfaces include physical NNIs or ENIs with spanning tree enabled, VLANs, and NNI or ENI port channels. The VLAN ID range is 1 to 4094. The port-channel range is 1 to 48. **Note**
Step 3	**spanning-tree mst pre-standard**	Specify that the port can send only prestandard BPDUs.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show spanning-tree mst interface** *interface-id*	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the port to its default setting, use the **no spanning-tree mst prestandard** interface configuration command.

EXAMPLE

This example shows how to configure a port to transmit only prestandard BPDUs:

```
Switch(config-if)# spanning-tree mst pre-standard
Switch(config-if)# end
```

Restarting the Protocol Migration Process

A switch running MSTP supports a built-in protocol migration mechanism that enables it to interoperate with legacy 802.1D switches. If this switch receives a legacy 802.1D configuration BPDU (a BPDU with the protocol version set to 0), it sends only 802.1D BPDUs on that port. An MSTP switch also can detect that a port is at the boundary of a region when it receives a legacy BPDU, an MST BPDU (Version 3) associated with a different region, or an RST BPDU (Version 2).

However, the switch does not automatically revert to the MSTP mode if it no longer receives 802.1D BPDUs because it cannot detect whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. A switch also might continue to assign a boundary role to a port when the switch to which it is connected has joined the region.

To restart the protocol migration process (force the renegotiation with neighboring switches) on the switch, use the **clear spanning-tree detected-protocols** privileged EXEC command.

To restart the protocol migration process on a specific interface, use the **clear spanning-tree detected-protocols interface** *interface-id* privileged EXEC command.

Verifying Configuration

Command	Purpose
show spanning-tree mst configuration	Display the MST region configuration.
show spanning-tree mst configuration digest	Display the MD5 digest included in the current MSTCI.
show spanning-tree mst *instance-id*	Display MST information for the specified instance.
show spanning-tree mst interface *interface-id*	Display MST information for the specified interface.

Configuration Example

This example shows how to enter MST configuration mode, map VLANs 10 to 20 to MST instance 1, name the region *region1*, set the configuration revision to 1, display the pending configuration, apply the changes, and return to global configuration mode:

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
```

```
Revision  1
Instance  Vlans Mapped
--------  ---------------------
0         1-9,21-4094
1         10-20
-------------------------------

Switch(config-mst)# exit
Switch(config)#
```

This example configures MST instance 0 as the root switch:

```
Switch(config)# spanning-tree mst 0 root primary
    mst 0 bridge priority set to 24576
    mst bridge max aging time unchanged at 20
    mst bridge hello time unchanged at 2
    mst bridge forward delay unchanged at 15
Switch(config)# end
Switch#
```

The following example shows how to increase the likelihood that spanning-tree instance 20 is chosen as the root-bridge on interface Ethernet 2/0:

```
Switch(config)# interface ethernet 2/0
Switch(config-if)# spanning-tree port-priority 20
Switch(config-if)#
```

This example shows how to set the interface path cost:

```
Switch(config)# interface fastethernet 4/4
Switch(config-if)# spanning-tree mst 0 cost 17031970
Switch(config-if)# end
```

This example shows how to set the switch priority:

```
Switch(config)# spanning-tree mst 0 priority 4096
Switch(config)# end
```

This example shows how to set the hello-time delay timer:

```
Switch(config)# spanning-tree mst hello-time 3
Switch(config)# end
```

This example shows how to set the forward-delay timer:

```
Switch(config)# spanning-tree mst forward-time 20
Switch(config)# end
```

This example shows how to set the max-age timer:

```
Switch(config)# spanning-tree mst max-age 40
Switch(config)# end
```

This example shows how to set the number of possible hops:

```
Switch(config)# spanning-tree mst max-hops 25
Switch(config)# end
```

This example shows how to configure the port as a point-to-point link:

```
Switch(config-if)# spanning-tree link-type point-to-point
Switch(config-if)# end
```

This example shows how to configure a port to transmit only prestandard BPDUs:

```
Switch(config-if)# spanning-tree mst pre-standard
Switch(config-if)# end
```

Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS LAN Switching Command Reference

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520 Switch	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

CHAPTER 13

Configuring Optional Spanning-Tree Features

This chapter describes how to configure optional spanning-tree features on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*. You can configure all of these features when your switch is running per-VLAN spanning-tree plus (PVST+). You can configure only the noted features when your switch is running the Multiple Spanning Tree Protocol (MSTP) or the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol. On the switch, STP is enabled by default on network node interfaces (NNIs). It is disabled by default, but can be enabled, on enhanced network interfaces (ENIs). User network interfaces (UNIs) on the switch do not participate in STP. UNIs and ENIs on which STP is not enabled immediately forward traffic when they are brought up.

For information on configuring the PVST+ and rapid PVST+, see Chapter 11, "Configuring STP." For information about the Multiple Spanning Tree Protocol (MSTP) and how to map multiple VLANs to the same spanning-tree instance, see Chapter 12, "Configuring MSTP."

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 13-14.

This chapter includes the following sections:

- Information About Optional Spanning-Tree Features, page 13-1
- Prerequisites, page 13-5
- Guidelines and Limitations, page 13-6
- Default Settings, page 13-6
- Configuring Optional Spanning-Tree Features, page 13-6
- Verifying Configuration, page 13-13
- Configuration Example, page 13-13
- Related Documents, page 13-14
- Feature History, page 13-14

Information About Optional Spanning-Tree Features

- Port Fast, page 13-2
- BPDU Guard, page 13-3
- BPDU Filtering, page 13-3

Port Fast

Port Fast immediately brings an STP port configured as an access or trunk port to the forwarding state from a blocking state, bypassing the listening and learning states.

Note By default, STP is enabled on NNIs and disabled on ENIs. UNIs do not support STP. If a port is a UNI, you can configure it as an STP port by changing the port type to NNI or ENI and entering the **port-type** {**nni** | **eni**} interface configuration command. For ENIs, you then need to enter the **spanning-tree** interface configuration command to configure the port as an STP port.

You can use Port Fast on STP ports connected to a single workstation or server, as shown in Figure 13-1, to allow those devices to immediately connect to the network, rather than waiting for the spanning tree to converge.

STP ports connected to a single workstation or server should not receive bridge protocol data units (BPDUs). An STP port with Port Fast enabled goes through the normal cycle of spanning-tree status changes when the switch is restarted.

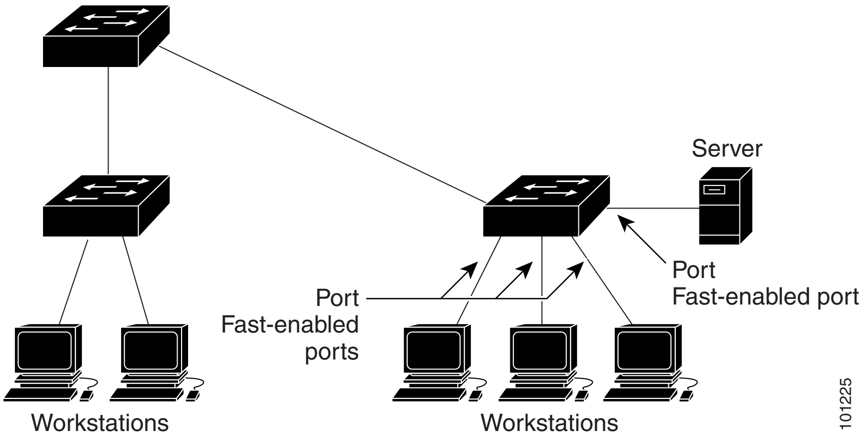
Note Because the purpose of Port Fast is to minimize the time interfaces must wait for spanning tree to converge, it is effective only when used on STP ports connected to end stations. If you enable Port Fast on an interface connecting to another switch, you risk creating a spanning-tree loop.

UNIs are typically customer-facing ports and do not participate in the spanning tree of the service provider. However, if you configure a customer-facing port as an ENI and enable spanning tree, the ENI could become the spanning tree root port unless you configure root guard on the port. See the "Root Guard" section on page 13-4. A customer-facing ENI with STP enabled participates in the same spanning tree as the service-provider facing NNI.

Note Exercise caution when enabling STP on a customer-facing ENI.

You can enable this feature by using the **spanning-tree portfast** interface configuration or the **spanning-tree portfast default** global configuration command.

Figure 13-1 Port Fast-Enabled Interfaces



BPDU Guard

The BPDU guard feature can be globally enabled on the switch or can be enabled per interface, but the feature operates with some differences.

At the global level, you enable BPDU guard on Port Fast-enabled STP ports by using the **spanning-tree portfast bpduguard default** global configuration command. Spanning tree shuts down STP ports that are in a Port Fast-operational state if any BPDU is received on those ports. In a valid configuration, Port Fast-enabled STP ports do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled port signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the interface in the error-disabled state.

At the interface level, you enable BPDU guard on any STP port by using the **spanning-tree bpduguard enable** interface configuration command without also enabling the Port Fast feature. When the STP port receives a BPDU, it is put in the error-disabled state.

The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

You can enable the BPDU guard feature for the entire switch or for an interface.

BPDU Filtering

The BPDU filtering feature can be globally enabled on the switch or can be enabled per interface, but the feature operates with some differences.

At the global level, you can enable BPDU filtering on Port Fast-enabled STP ports by using the **spanning-tree portfast bpdufilter default** global configuration command. This command prevents interfaces that are in a Port Fast-operational state from sending or receiving BPDUs. The interfaces still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to these ports do not receive BPDUs. If a BPDU is received on a Port Fast-enabled STP port, the interface loses its Port Fast-operational status, and BPDU filtering is disabled.

At the interface level, you can enable BPDU filtering on any STP port by using the **spanning-tree bpdufilter enable** interface configuration command without also enabling the Port Fast feature. This command prevents the interface from sending or receiving BPDUs.

Caution Enabling BPDU filtering on an STP port is the same as disabling spanning tree on it and can result in spanning-tree loops.

You can enable the BPDU filtering feature for the entire switch or for an STP port.

EtherChannel Guard

You can use EtherChannel guard to detect an EtherChannel misconfiguration between the switch and a connected device. A misconfiguration can occur if the switch STP ports are configured in an EtherChannel, but the interfaces on the other device are not. A misconfiguration can also occur if the channel parameters are not the same at both ends of the EtherChannel. For EtherChannel configuration guidelines, see the "EtherChannel Configuration Guidelines section of the "Configuring EtherChannels and Link State Tracking" chapter in the *High Availability and Redundancy Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.

If the switch detects a misconfiguration on the other device, EtherChannel guard places the switch STP ports in the error-disabled state, and displays an error message.

You can enable this feature by using the **spanning-tree etherchannel guard misconfig** global configuration command.

Root Guard

The Layer 2 network of a service provider (SP) can include many connections to switches that are not owned by the SP. In such a topology, the spanning tree can reconfigure itself and select a *customer switch* as the root switch, as shown in Figure 13-2. You can avoid this situation by enabling root guard on SP switch interfaces that connect to switches in your customer's network. If spanning-tree calculations cause an interface in the customer network to be selected as the root port, root guard then places the interface in the root-inconsistent (blocked) state to prevent the customer's switch from becoming the root switch or being in the path to the root.

If a switch outside the SP network becomes the root switch, the interface is blocked (root-inconsistent state), and spanning tree selects a new root switch. The customer's switch does not become the root switch and is not in the path to the root.

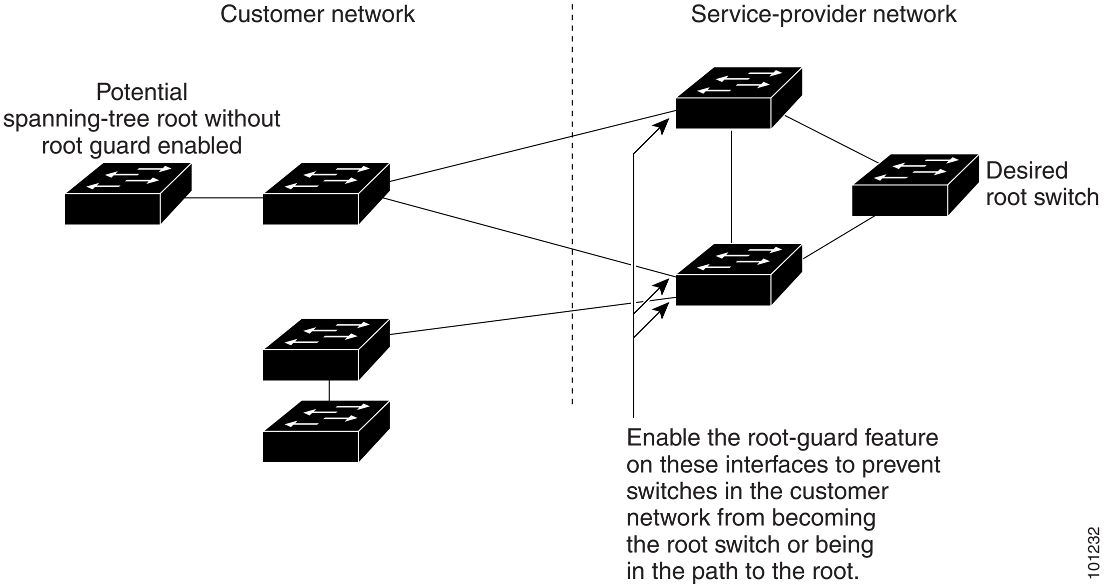
If the switch is operating in multiple spanning-tree (MST) mode, root guard forces the interface to be a designated port. If a boundary port is blocked in an internal spanning-tree (IST) instance because of root guard, the interface also is blocked in all MST instances. A boundary port is an interface that connects to a LAN, the designated switch of which is either an 802.1D switch or a switch with a different MST region configuration.

Root guard enabled on an interface applies to all the VLANs to which the interface belongs. VLANs can be grouped and mapped to an MST instance.

You can enable this feature by using the **spanning-tree guard root** interface configuration command.

Caution Misuse of the root-guard feature can cause a loss of connectivity.

Figure 13-2 Root Guard in a Service-Provider Network


Customer network
Service-provider network
Potential spanning-tree root without root guard enabled
Desired root switch
Enable the root-guard feature on these interfaces to prevent switches in the customer network from becoming the root switch or being in the path to the root.
101232

Loop Guard

You can use loop guard to prevent alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. This feature is most effective when it is enabled on the entire switched network. Loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send BPDUs on root or alternate ports.

You can enable this feature by using the **spanning-tree loopguard default** global configuration command.

When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send BPDUs on root or alternate ports.

When the switch is operating in MST mode, BPDUs are not sent on nonboundary ports only if the interface is blocked by loop guard in all MST instances. On a boundary port, loop guard blocks the interface in all MST instances.

Prerequisites

- Be familiar with the information in the "Information About Optional Spanning-Tree Features" section on page 13-1 and "Guidelines and Limitations" section on page 13-6.
- Ensure that your network strategy and planning for your network are complete.
- Ensure that STP is enabled.

Guidelines and Limitations

You can configure PortFast, BPDU guard, BPDU filtering, EtherChannel guard, root guard, or loop guard if your switch is running PVST+, rapid PVST+, or MSTP.

Optional spanning-tree configuration commands are not supported on UNIs or on ENIs on which STP has not been enabled.

Default Settings

Only NNIs or ENIs with STP enabled participate in STP on the switch. UNIs and ENIs that have not been configured for STP are always in the forwarding state.

Feature	Default Setting
Port Fast, BPDU filtering, BPDU guard	Globally disabled (unless they are individually configured per STP port).
EtherChannel guard	Globally enabled.
Root guard	Disabled on all STP ports.
Loop guard	Disabled on all STP ports.

Configuring Optional Spanning-Tree Features

This section includes the following topics:

- Enabling Port Fast, page 13-6 (optional)
- Enabling BPDU Guard, page 13-8 (optional)
- Enabling BPDU Filtering, page 13-9 (optional)
- Enabling EtherChannel Guard, page 13-10 (optional)
- Enabling Root Guard, page 13-11 (optional)
- Enabling Loop Guard, page 13-12 (optional)

Enabling Port Fast

An STP port with the Port Fast feature enabled is moved directly to the spanning-tree forwarding state without waiting for the standard forward-time delay.

You can enable this feature if your switch is running PVST+, rapid PVST+, or MSTP. This procedure is optional.

Note You can use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking STP ports.

BEFORE YOU BEGIN

Caution Use Port Fast *only* when connecting a single end station to an access or trunk port. Enabling this feature on an interface connected to a switch or hub could prevent spanning tree from detecting and disabling loops in your network, which could cause broadcast storms and address-learning problems.

Caution Make sure that there are no loops in the network between the trunk port and the workstation or server before you enable Port Fast on a trunk port.

If the interface is a UNI, before you enable Port Fast, you must change the port type to NNI or ENI to enable STP:

- Enter the **port-type nni** interface configuration command to change the port to an NNI with STP enabled by default.
- Or enter the **port-type eni** and **spanning-tree** interface configuration commands to configure the port as an ENI STP port.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify an STP interface to configure, and enter interface configuration mode.
Step 3	**spanning-tree portfast** [**trunk**]	Enable Port Fast on an access port connected to a single workstation or server. By specifying the **trunk** keyword, you can enable Port Fast on a trunk port. **Note** To enable Port Fast on trunk ports, you must use the **spanning-tree portfast trunk** interface configuration command. The **spanning-tree portfast** command does not work on trunk ports. By default, Port Fast is disabled on all STP ports.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show spanning-tree interface** *interface-id* **portfast**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable the Port Fast feature, use the **spanning-tree portfast disable** interface configuration command.

EXAMPLE

This example configures Port Fast on an access port:

```
Switch(config)# interface ethernet 2/0
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
```

Enabling BPDU Guard

When you globally enable BPDU guard on ports that are Port Fast-enabled (the ports are in a Port Fast-operational state), spanning tree continues to run on the ports. They remain up unless they receive a BPDU.

In a valid configuration, Port Fast-enabled interfaces do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled interface signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the interface in the error-disabled state. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

You also can use the **spanning-tree bpduguard enable** interface configuration command to enable BPDU guard on any STP port without also enabling the Port Fast feature. When the interface receives a BPDU, it is put in the error-disabled state.

You can enable the BPDU guard feature if your switch is running PVST+, rapid PVST+, or MSTP. This procedure is optional.

BEFORE YOU BEGIN

Caution Configure Port Fast only on STP ports that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation.

If the interface is a UNI, before you enable Port Fast, you must change the port type to NNI or ENI to enable STP:

- Enter the **port-type nni** interface configuration command to change the port to an NNI with STP enabled by default.
- Or enter the **port-type eni** and **spanning-tree** interface configuration commands to configure the port as an ENI STP port.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree portfast bpduguard default**	Globally enable BPDU guard. (By default, BPDU guard is disabled.) **Note** Globally enabling BPDU guard enables it only on STP ports; the command has no effect on ports that are not running STP.
Step 3	**interface** *interface-id*	Specify the interface connected to an end station, and enter interface configuration mode.
Step 4	**spanning-tree portfast**	Enable the Port Fast feature.
Step 5	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable BPDU guard, use the **no spanning-tree portfast bpduguard default** global configuration command.

You can override the setting of the **no spanning-tree portfast bpduguard default** global configuration command by using the **spanning-tree bpduguard enable** interface configuration command on an STP port.

EXAMPLE

This example shows how to enable BPDU guard by default:

```
Switch(config)# spanning-tree portfast bpduguard default
Switch(config)# interface ethernet 2/0
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
```

Enabling BPDU Filtering

When you globally enable BPDU filtering on Port Fast-enabled STP ports, it prevents interfaces that are in a Port Fast-operational state from sending or receiving BPDUs. The interfaces still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to these interfaces do not receive BPDUs. If a BPDU is received on a Port Fast-enabled STP port, the interface loses its Port Fast-operational status, and BPDU filtering is disabled.

You can also use the **spanning-tree bpdufilter enable** interface configuration command to enable BPDU filtering on any STP port without also enabling the Port Fast feature. This command prevents the STP port from sending or receiving BPDUs.

You can enable the BPDU filtering feature if your switch is running PVST+, rapid PVST+, or MSTP. This procedure is optional.

BEFORE YOU BEGIN

⚠ **Caution** Configure Port Fast only on STP ports that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation.

⚠ **Caution** Enabling BPDU filtering on an STP port is the same as disabling spanning tree on it and can result in spanning-tree loops.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree portfast bpdufilter default**	Globally enable BPDU filtering. (By default, BPDU filtering is disabled.) **Note** Globally enabling BPDU filtering enables it only on STP ports; the command has no effect on UNIs or ENIs on which STP is not enabled.
Step 3	**interface** *interface-id*	Specify the interface connected to an end station, and enter interface configuration mode. If the interface is a UNI, before you enable Port Fast, you must change the port type to NNI or ENI to enable STP: • Enter the **port-type nni** interface configuration command to change the port to an NNI with STP enabled by default. • Or enter the **port-type eni** and **spanning-tree** interface configuration commands to configure the port as an ENI STP port.
Step 4	**spanning-tree portfast**	Enable the Port Fast feature.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable BPDU filtering, use the **no spanning-tree portfast bpdufilter default** global configuration command.

You can override the setting of the **no spanning-tree portfast bpdufilter default** global configuration command by using the **spanning-tree bpdufilter enable** interface configuration command on an STP port.

EXAMPLE

This example shows how to enable BPDU filtering by default:

```
Switch(config)# spanning-tree portfast bpdufilter default
Switch(config)# interface ethernet 2/0
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
```

Enabling EtherChannel Guard

You can enable EtherChannel guard to detect an EtherChannel misconfiguration if your switch is running PVST+, rapid PVST+, or MSTP. This procedure is optional.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree etherchannel guard misconfig**	Enable EtherChannel guard.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree summary**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable the EtherChannel guard feature, use the **no spanning-tree etherchannel guard misconfig** global configuration command.

You can use the **show interfaces status err-disabled** privileged EXEC command to show which switch STP ports are disabled because of an EtherChannel misconfiguration. On the remote device, you can enter the **show etherchannel summary** privileged EXEC command to verify the EtherChannel configuration.

After the configuration is corrected, enter the **shutdown** and **no shutdown** interface configuration commands on the port-channel interfaces that were misconfigured.

EXAMPLE

This example shows how to enable EtherChannel guard:

```
Switch(config)# spanning-tree etherchannel guard misconfig
Switch(config)# end
```

Enabling Root Guard

Root guard enabled on an STP port applies to all the VLANs to which the port belongs.

You can enable this feature if your switch is running PVST+, rapid PVST+, or MSTP. This procedure is optional.

BEFORE YOU BEGIN

Note You cannot enable both root guard and loop guard at the same time.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify an interface to configure, and enter interface configuration mode. If the interface is a UNI, before you enable root guard, you must change the port type to NNI or ENI to enable STP: • Enter the **port-type nni** interface configuration command to change the port to an NNI with STP enabled by default. • Or enter the **port-type eni** and **spanning-tree** interface configuration commands to configure the port as an ENI STP port.
Step 3	**spanning-tree guard root**	Enable root guard on the STP port. By default, root guard is disabled on all interfaces.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable root guard, use the **no spanning-tree guard** interface configuration command.

EXAMPLE

This example shows how to enable root guard:

```
Switch(config-if)# spanning-tree guard root
Switch(config-if)# end
```

Enabling Loop Guard

You can use loop guard to prevent alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. This feature is most effective when it is configured on the entire switched network. Loop guard operates only on STP ports that are considered point-to-point by the spanning tree.

You can enable this feature if your switch is running PVST+, rapid PVST+, or MSTP. This procedure is optional.

BEFORE YOU BEGIN

Note You cannot enable both loop guard and root guard at the same time.

DETAILED STEPS

	Command	Purpose
Step 1	**show spanning-tree active** or **show spanning-tree mst**	Verify which interfaces are alternate or root ports.
Step 2	**configure terminal**	Enter global configuration mode.
Step 3	**spanning-tree loopguard default**	Enable loop guard. By default, loop guard is disabled.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To globally disable loop guard, use the **no spanning-tree loopguard default** global configuration command. You can override the setting of the **no spanning-tree loopguard default** global configuration command by using the **spanning-tree guard loop** interface configuration command on an NNI.

EXAMPLE

This example shows how to enable loop guard:

```
Switch(config)# spanning-tree loopguard default
Switch(config)# end
```

Verifying Configuration

Command	Purpose
show spanning-tree active	Display spanning-tree information on active interfaces only.
show spanning-tree detail	Display a detailed summary of interface information.
show spanning-tree interface *interface-id*	Display spanning-tree information for the specified interface.
show spanning-tree mst interface *interface-id*	Display MST information for the specified interface.
show spanning-tree summary [**totals**]	Display a summary of interface states or displays the total lines of the spanning-tree state section.

You can clear spanning-tree counters by using the **clear spanning-tree** [**interface** *interface-id*] privileged EXEC command.

Configuration Example

This example configures Port Fast on an access port:

```
Switch(config)# interface ethernet 2/0
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
```

This example shows how to enable BPDU guard by default:

```
Switch(config)# spanning-tree portfast bpduguard default
Switch(config)# interface ethernet 2/0
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
```

This example shows how to enable BPDU filtering by default:

```
Switch(config)# spanning-tree portfast bpdufilter default
Switch(config)# interface ethernet 2/0
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
```

This example shows how to enable EtherChannel guard:

```
Switch(config)# spanning-tree etherchannel guard misconfig
Switch(config)# end
```

This example shows how to enable root guard:

```
Switch(config-if)# spanning-tree guard root
Switch(config-if)#
```

This example shows how to enable loop guard:

```
Switch(config)# spanning-tree loopguard default
Switch(config)# end
```

Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS LAN Switching Command Reference
- High Availability and Redundancy Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520 Switch	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

CHAPTER 14

Configuring Resilient Ethernet Protocol

This chapter describes how to use Resilient Ethernet Protocol (REP) on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*. REP is a Cisco proprietary protocol that provides an alternative to Spanning Tree Protocol (STP) to control network loops, respond to link failures, and improve convergence time. REP controls a group of ports connected in a segment, ensures that the segment does not create any bridging loops, and responds to link failures within the segment. REP provides a basis for constructing more complex networks and supports VLAN load balancing.

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 14-16.

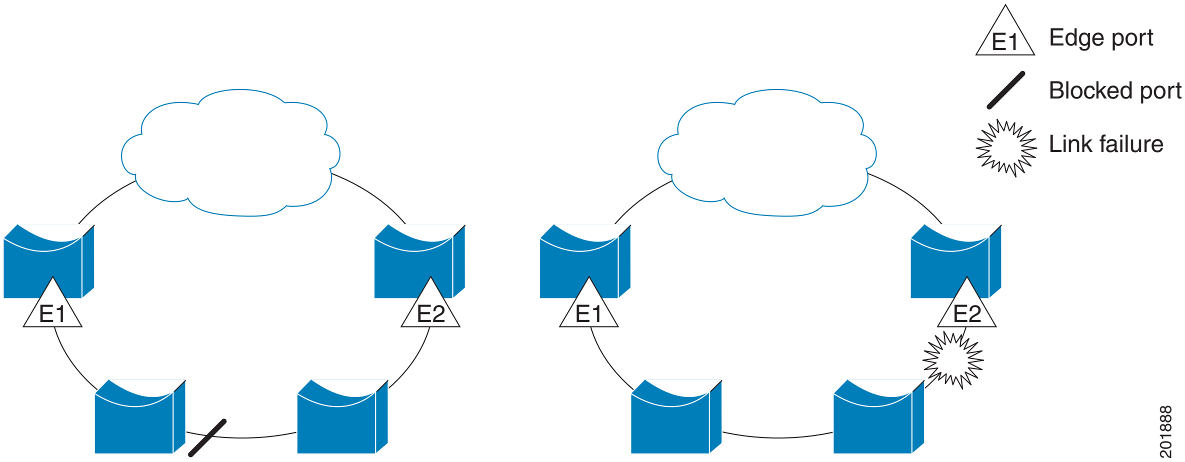
This chapter includes the following sections:

Information About REP

A REP segment is a chain of ports connected to each other and configured with a segment ID. Each segment consists of standard (nonedge) segment ports and two user-configured edge ports. A switch can have only two ports belonging to the same segment, and each segment port can have only one external neighbor. A segment can go through a shared medium, but on any link, only two ports can belong to the same segment. REP is supported only on Layer 2 trunk interfaces.

Figure 14-1 shows an example of a segment consisting of six ports spread across four switches. Ports E1 and E2 are configured as edge ports. When all ports are operational (as in the segment on the left), a single port is blocked, shown by the diagonal line. When there is a network failure, as shown in the diagram on the right, the blocked port returns to the forwarding state to minimize network disruption.

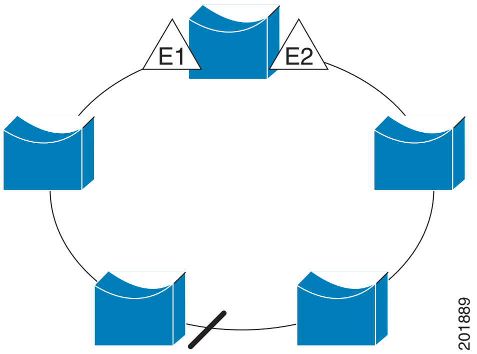
Figure 14-1 REP Open Segments



The segment shown in Figure 14-1 is an open segment; there is no connectivity between the two edge ports. The REP segment cannot cause a bridging loop, and you can safely connect the segment edges to any network. All hosts connected to switches inside the segment have two possible connections to the rest of the network through the edge ports, but only one connection is accessible at any time. If a host cannot access its usual gateway because of a failure, REP unblocks all ports to ensure that connectivity is available through the other gateway.

The segment shown in Figure 14-2, with both edge ports located on the same switch, is a ring segment. In this configuration, there is connectivity between the edge ports through the segment. With this configuration, you can create a redundant connection between any two switches in the segment.

Figure 14-2 REP Ring Segment



REP segments have these characteristics:

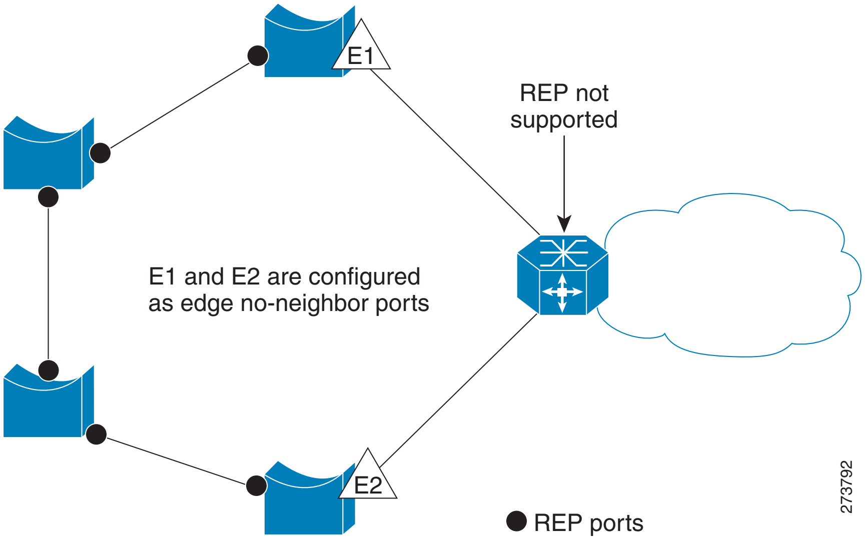
- If all ports in the segment are operational, one port (referred to as the *alternate* port) is in the blocked state for each VLAN.
- If VLAN load balancing is configured, two ports in the segment control the blocked state of VLANs.

- If one or more ports in a segment is not operational, causing a link failure, all ports forward traffic on all VLANs to ensure connectivity.
- In case of a link failure, the alternate ports are unblocked as quickly as possible. When the failed link comes back up, a logically blocked port per VLAN is selected with minimal disruption to the network.

You can construct almost any type of network based on REP segments. REP also supports VLAN load-balancing, controlled by the primary edge port but occurring at any port in the segment.

In access ring topologies, the neighboring switch might not support REP, as shown in Figure 14-3. In this case, you can configure the non-REP facing ports (E1 and E2) as edge no-neighbor ports. These ports inherit all properties of edge ports, and you can configure them the same as any edge port, including configuring them to send STP or REP topology change notices to the aggregation switch. In this case the STP topology change notice (TCN) that is sent is a multiple spanning-tree (MST) STP message.

Figure 14-3 Edge No-Neighbor Ports



REP has these limitations:

- You must configure each segment port; an incorrect configuration can cause forwarding loops in the networks.
- REP can manage only a single failed port within the segment; multiple port failures within the REP segment cause loss of network connectivity.
- You should configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

Link Integrity

REP does not use an end-to-end polling mechanism between edge ports to verify link integrity. It implements local link failure detection. The REP Link Status Layer (LSL) detects its REP-aware neighbor and establishes connectivity within the segment. All VLANs are blocked on an interface until it detects the neighbor. After the neighbor is identified, REP determines which neighbor port should become the alternate port and which ports should forward traffic.

Each port in a segment has a unique port ID. The port ID format is similar to that used by the spanning tree algorithm: a port number (unique on the bridge), associated to a MAC address (unique in the network). When a segment port is coming up, its LSL starts sending packets that include the segment ID and the port ID. The port is declared operational after it performs a three-way handshake with a neighbor in the same segment.

A segment port does not become operational if:

- No neighbor has the same segment ID.
- More than one neighbor has the same segment ID.
- The neighbor does not acknowledge the local port as a peer.

Each port creates an adjacency with its immediate neighbor. After the neighbor adjacencies are created, the ports negotiate to determine one blocked port for the segment, the alternate port. All other ports become unblocked. By default, REP packets are sent to a BPDU class MAC address. The packets can also be sent to the Cisco multicast address, which is used only to send blocked port advertisement (BPA) messages when there is a failure in the segment. The packets are dropped by devices not running REP.

Fast Convergence

Because REP runs on a physical link basis and not a per-VLAN basis, only one hello message is required for all VLANs, reducing the load on the protocol. We recommend that you create VLANs consistently on all switches in a given segment and configure the same allowed VLANs on the REP trunk ports. To avoid the delay introduced by relaying messages in software, REP also allows some packets to be flooded to a regular multicast address. These messages operate at the hardware flood layer (HFL) and are flooded to the whole network, not just the REP segment. Switches that do not belong to the segment treat them as data traffic. You can control flooding of these messages by configuring a dedicated administrative VLAN for the whole domain.

The estimated convergence recovery time on fiber interfaces is less than 200 ms for the local segment with 200 VLANs configured. Convergence for VLAN load balancing is 300 ms or less.

VLAN Load Balancing

One edge port in the REP segment acts as the primary edge port; the other as the secondary edge port. The primary edge port always participates in VLAN load balancing in the segment. REP VLAN balancing is achieved by blocking some VLANs at a configured alternate port and all other VLANs at the primary edge port. When you configure VLAN load balancing, you can specify the alternate port in one of three ways:

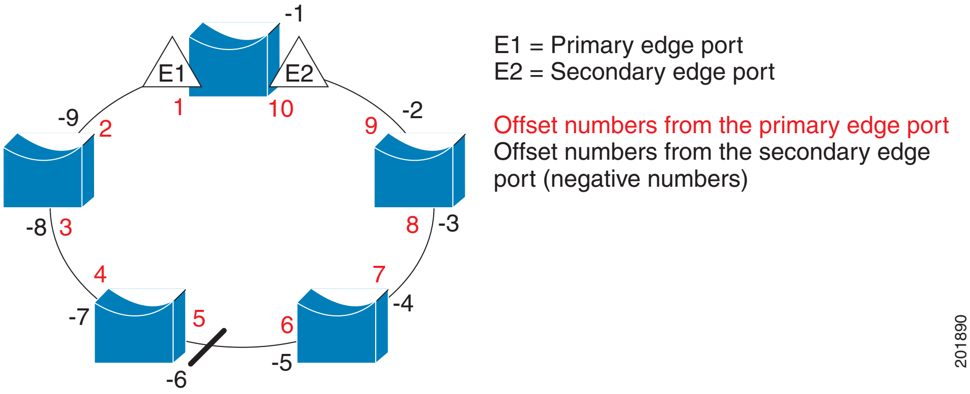
- Enter the port ID of the interface. To identify the port ID of a port in the segment, enter the **show interface rep detail** interface configuration command for the port.
- Enter the neighbor offset number of a port in the segment, which identifies the downstream neighbor port of an edge port. The neighbor offset number range is –256 to +256; a value of 0 is invalid. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors.

Note You configure offset numbers on the primary edge port by identifying the downstream position from the primary (or secondary) edge port. You would never enter an offset value of 1 because that is the offset number of the primary edge port itself.

Figure 14-4 shows neighbor offset numbers for a segment where E1 is the primary edge port and E2 is the secondary edge port. The red numbers inside the ring are numbers offset from the primary edge port; the black numbers outside the ring show the offset numbers from the secondary edge port. Note that you can identify all ports (except the primary edge port) by either a positive offset number (downstream position from the primary edge port) or a negative offset number (downstream position from the secondary edge port). If E2 became the primary edge port, its offset number would then be 1, and E1 would be -1.

- By entering the **preferred** keyword to select the port that you previously configured as the preferred alternate port with the **rep segment** *segment-id* **preferred** interface configuration command.

Figure 14-4 Neighbor Offset Numbers in a Segment


-1
E1
E2
1
10
-9
2
9
-2
-8
3
8
-3
4
7
-7
5
6
-4
-6
-5
E1 = Primary edge port
E2 = Secondary edge port
Offset numbers from the primary edge port
Offset numbers from the secondary edge port (negative numbers)
201890

When the REP segment is complete, all VLANs are blocked. When you configure VLAN load balancing, you must also configure triggers in one of two ways:

- Manually trigger VLAN load balancing at any time by entering the **rep preempt segment** *segment-id* privileged EXEC command on the switch that has the primary edge port.
- Configure a preempt delay time by entering the **rep preempt delay** *seconds* interface configuration command. After a link failure and recovery, VLAN load balancing begins after the configured preemption time period elapses. Note that the delay timer restarts if another port fails before the time has elapsed.

Note When VLAN load balancing is configured, it does not start working until triggered by either manual intervention or a link failure and recovery.

When VLAN load balancing is triggered, the primary edge port sends a message to alert all interfaces in the segment about the preemption. When the secondary port receives the message, it is reflected into the network to notify the alternate port to block the set of VLANs specified in the message and to notify the primary edge port to block the remaining VLANs.

You can also configure a particular port in the segment to block all VLANs. Only the primary edge port initiates VLAN load balancing, which is not possible if the segment is not terminated by an edge port on each end. The primary edge port determines the local VLAN load balancing configuration.

Reconfigure the primary edge port to reconfigure load balancing. When you change the load balancing configuration, the primary edge port again waits for the **rep preempt segment** command or for the configured preempt delay period after a port failure and recovery before executing the new configuration. If you change an edge port to a regular segment port, the existing VLAN load balancing status does not change. Configuring a new edge port might cause a new topology configuration.

Spanning Tree Interaction

REP does not interact with STP or with the Flex Link feature, but can coexist with both. A port that belongs to a segment is removed from spanning tree control and STP BPDUs are not accepted or sent from segment ports.

To migrate from an STP ring configuration to REP segment configuration, begin by configuring a single port in the ring as part of the segment, and continue by configuring contiguous ports to minimize the number of segments. Each segment always contains a blocked port, so multiple segments means multiple blocked ports and a potential loss of connectivity. When the segment has been configured in both directions to the edge ports, you then configure the edge ports.

REP Ports

Ports in REP segments are Failed, Open, or Alternate.

- A port configured as a regular segment port starts as a failed port.
- After the neighbor adjacencies are determined, the port changes to alternate port state, blocking all VLANs on the interface. Blocked port negotiations occur and when the segment settles, one blocked port remains in the alternate role, and all other ports become open ports.
- When a failure occurs in a link, all ports move to the open state. When the alternate port receives the failure notification, it changes to the open state, forwarding all VLANs.

A regular segment port converted to an edge port, or an edge port converted to a regular segment port, does not always result in a topology change. If you convert an edge port into a regular segment port, VLAN load balancing is not implemented unless it has been configured. For VLAN load balancing, you must configure two edge ports in the segment.

A segment port that is reconfigured as a spanning tree port restarts according the spanning tree configuration. By default, this is a designated blocking port. If PortFast is configured or if STP is disabled, the port goes into the forwarding state.

Prerequisites

Be familiar with the information in the "Information About REP" section on page 14-1 and "Guidelines and Limitations" section on page 14-6.

Guidelines and Limitations

Follow these guidelines when configuring REP:

- We recommend that you begin by configuring one port and then configure the contiguous ports to minimize the number of segments and the number of blocked ports.
- If more than two ports in a segment fail when no external neighbors are configured, one port goes into a forwarding state for the data path to help maintain connectivity during configuration. In the **show rep interface** privileged EXEC command output, the Port Role for this port shows as *Fail Logical Open*; the Port Role for the other failed port shows as *Fail No Ext Neighbor*. When the external neighbors for the failed ports are configured, the ports go through the alternate port state transitions and eventually go to an open state or remain as the alternate port, based on the alternate port election mechanism.

- REP ports must be Layer 2 trunk ports.
- Be careful when configuring REP through a Telnet connection. Because REP blocks all VLANs until another REP interface sends a message to unblock the VLAN, you might lose connectivity to the switch if you enable REP in a Telnet session that accesses the switch through the REP interface.
- You cannot run REP and STP or REP and Flex Links on the same segment or interface.
- If you connect an STP network to the REP segment, be sure that the connection is at the segment edge. An STP connection that is not at the edge could cause a bridging loop because STP does not run on REP segments. All STP BPDUs are dropped at REP interfaces.
- You must configure all trunk ports in the segment with the same set of allowed VLANs, or a misconfiguration occurs.
- REP ports follow these rules:
  - There is no limit to the number of REP ports on a switch; however, only two ports on a switch can belong to the same REP segment.
  - If only one port on a switch is configured in a segment, the port should be an edge port.
  - If two ports on a switch belong to the same segment, they must be both edge ports, both regular segment ports, or one regular port and one edge no-neighbor port. An edge port and regular segment port on a switch cannot belong to the same segment.
  - If two ports on a switch belong to the same segment and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.
- REP interfaces come up and remain in a blocked state until notified that it is safe to unblock. You need to be aware of this to avoid sudden connection losses.
- REP sends all LSL PDUs in untagged frames on the native VLAN. The BPA message sent to the Cisco multicast address is sent on the administration VLAN, which is VLAN 1 by default.
- You can configure how long a REP interface remains up without receiving a hello from a neighbor. You can use the **rep lsl-age-time**r *value* interface configuration command to set the time from 120 ms to 10000 ms. The LSL hello timer is then set to the age-timer value divided by three. In normal operation, three LSL hellos are sent before the age timer on the peer switch expires and searches for hello messages.
  - The LSL age-timer range changed from 3000 to 10000 ms in 500-ms increments to 120 ms to 10000 ms in 40-ms increments. If the REP neighbor device is not running Cisco IOS Release 12.2(52)SE or later, you must use the shorter time range because the device will not accept values out of the previous range.
  - EtherChannel port channel interfaces do not support LSL age-timer values less than 1000 ms. If you try to configure a value less than 1000 ms on a port channel, you receive an error message and the command is rejected.
- REP ports cannot be configured as one of these port types:
  - SPAN destination port
  - Private VLAN port
  - Tunnel port
  - Access port
- REP ports must be network node interfaces (NNI). User-network interfaces (UNIs) or enhanced network interfaces (ENIs) cannot be REP ports.
- REP is supported on EtherChannels, but not on an individual port that belongs to an EtherChannel.

- There is a maximum of 64 REP segments per switch.

Default Settings

REP is disabled on all interfaces. When enabled, the interface is a regular segment port unless it is configured as an edge port.

When REP is enabled, the sending of segment topology change notices (STCNs) is disabled, all VLANs are blocked, and the administrative VLAN is VLAN 1.

When VLAN load balancing is enabled, the default is manual preemption with the delay timer disabled. If VLAN load balancing is not configured, the default after manual preemption is to block all VLANs at the primary edge port.

Configuring REP

A segment is a collection of ports connected one to the other in a chain and configured with a segment ID. To configure REP segments, you configure the REP administrative VLAN (or use the default VLAN 1) and then add the ports to the segment using interface configuration mode. You should configure two edge ports in the segment, one as the primary edge port and the other, by default, the secondary edge port. A segment has only one primary edge port. If you configure two ports in a segment as the primary edge port, for example ports on different switches, the REP selects one to serve as the segment primary edge port. You can also optionally configure where to send segment topology change notices (STCNs) and VLAN load balancing messages.

This section includes the following topics:

Configuring the REP Administrative VLAN

To avoid the delay introduced by relaying messages in software for link-failure or VLAN-blocking notification during load balancing, REP floods packets at the hardware flood layer (HFL) to a regular multicast address. These messages are flooded to the whole network, not just the REP segment. You can control flooding of these messages by configuring an administrative VLAN for the whole domain.

BEFORE YOU BEGIN

Follow these guidelines when configuring the REP administrative VLAN:

- If you do not configure an administrative VLAN, the default is VLAN 1.
- There can be only one administrative VLAN on a switch and on a segment. However, this is not enforced by software.
- The administrative VLAN cannot be the RSPAN VLAN.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**rep admin vlan** *vlan-id*	Specify the administrative VLAN. The range is 2 to 4094. The default is VLAN 1. To set the admin VLAN to 1, enter the **no rep admin vlan** global configuration command.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show interface** [*interface-id*] **rep detail**	Verify the configuration on one of the REP interfaces.
Step 5	**copy running-config startup config**	(Optional) Save your entries in the switch startup configuration file.

EXAMPLE

This example shows how to configure the administrative VLAN as VLAN 100 and to verify the configuration by entering the **show interface rep detail** command on one of the REP interfaces:

```
Switch# configure terminal
Switch (conf)# rep admin vlan 100
Switch (conf-if)# end

Switch# show interface gigabitethernet0/1 rep detail
GigabitEthernet0/1 REP enabled
Segment-id: 2 (Edge)
PortID: 00010019E7144680
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 0002001121A2D5800E4D
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 100
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 3322, tx: 1722
HFL PDU rx: 32, tx: 5
BPA TLV rx: 16849, tx: 508
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 118, tx: 118
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 4214, tx: 4190
```

Configuring REP Interfaces

For REP operation, you need to enable it on each segment interface and to identify the segment ID. This step is required and must be done before other REP configuration. You must also configure a primary and secondary edge port on each segment. All other steps are optional.

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 14-6.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface, and enter interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface). The port-channel range is 1 to 48.
Step 3	**port-type nni**	Configure the port as a network node interface (NNI).
Step 4	**switchport mode trunk**	Configure the interface as a Layer 2 trunk port.
Step 5	**rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]	Enable REP on the interface, and identify a segment number. The segment ID range is from 1 to 1024. These optional keywords are available. **Note** You must configure two edge ports, including one primary edge port for each segment. • Enter **edge** to configure the port as an edge port. Enter **edge** without the **primary** keyword to configure the port as the secondary edge port. Each segment has only two edge ports. • (Optional) Enter **no-neighbor** to configure a port with no external REP neighbors as an edge port. The port inherits all properties of edge ports, and you can configure them the same as any edge port. • (Optional) On an edge port, enter **primary** to configure the port as the primary edge port, the port on which you can configure VLAN load balancing. **Note** Although each segment can have only one primary edge port, if you configure edge ports on two different switches and enter the **primary** keyword on both switches, the configuration is allowed. However, REP selects only one of these ports as the segment primary edge port. You can identify the primary edge port for a segment by entering the **show rep topology** privileged EXEC command. • (Optional) Enter **preferred** to set the port as the preferred alternate port or the preferred port for VLAN load balancing. **Note** Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.

	Command	Purpose
Step 6	**rep stcn** {**interface** *interface-id* | **segment** *id-list* | **stp**}	(Optional) Configure the edge port to send segment topology change notices (STCNs). • Enter **interface** *interface-id* to designate a physical interface or port channel to receive STCNs. • Enter **segment** *id-list* to identify one or more segments to receive STCNs. The range is 1 to 1024. • Enter **stp** to send STCNs to STP networks.
Step 7	**rep block port** {**id** *port-id* | *neighbor_offset* | **preferred**} **vlan** {*vlan-list* | **all**}	(Optional) Configure VLAN load balancing on the primary edge port, identify the REP alternate port, and configure the VLANs to be blocked on the alternate port. • Enter the **id** *port-id* to identify the alternate port by port ID. The port ID is automatically generated for each port in the segment. You can view interface port IDs by entering the **show interface** *interface-id* **rep** [**detail**] privileged EXEC command. • Enter a *neighbor_offset* number to identify the alternate port as a downstream neighbor from an edge port. The range is from –256 to 256, with negative numbers identifying the downstream neighbor from the secondary edge port. A value of **0** is invalid. Enter **-1** to identify the secondary edge port as the alternate port. See Figure 14-4 on page 14-5 for an example of neighbor offset numbering. **Note** Because you enter this command at the primary edge port (offset number 1), you would never enter an offset value of 1 to identify an alternate port. • Enter **preferred** to select the regular segment port previously identified as the preferred alternate port for VLAN load balancing. • Enter **vlan** *vlan-list* to block one VLAN or a range of VLANs. • Enter **vlan all** to block all VLANs. **Note** Enter this command only on the REP primary edge port.
Step 8	**rep preempt delay** *seconds*	(Optional) You must enter this command and configure a preempt time delay if you want VLAN load balancing to automatically trigger after a link failure and recovery. The time delay range is 15 to 300 seconds. The default is manual preemption with no time delay. **Note** Enter this command only on the REP primary edge port.

	Command	Purpose
Step 9	**rep lsl-age-timer** *value*	(Optional) Configure a time (in milliseconds) for which the REP interface remains up without receiving a hello from a neighbor. The range is from 120 to 10000 ms in 40-ms increments; the default is 5000 ms (5 seconds). **Note** If the neighbor device is not running Cisco IOS Release 12.2(52)SE or later, it will only accept values from 3000 to 10000 ms in 500 ms increments. EtherChannel port channel interfaces do not support LSL age-timer values less than 1000 ms.
Step 10	**end**	Return to privileged EXEC mode.
Step 11	**show interface** [*interface-id*] **rep** [**detail**]	Verify the REP interface configuration.
Step 12	**copy running-config startup config**	(Optional) Save your entries in the switch startup configuration file.

Enter the **no** form of each command to return to the default configuration. Enter the **show rep topology** privileged EXEC command to see which port in the segment is the primary edge port.

EXAMPLE

This example shows how to configure an interface as the primary edge port for segment 1, to send STCNs to segments 2 through 5, and to configure the alternate port as the port with port ID 0009001818D68700 to block all VLANs after a preemption delay of 60 seconds after a segment port failure and recovery. The interface is configured to remain up for 6000 milliseconds without receiving a hello from a neighbor.

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet0/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep stcn segment 2-5
Switch (conf-if)# rep block port 0009001818D68700 vlan all
Switch (conf-if)# rep preempt delay 60
Switch (conf-if)# rep lsl-age-timer 6000
Switch (conf-if)# end
```

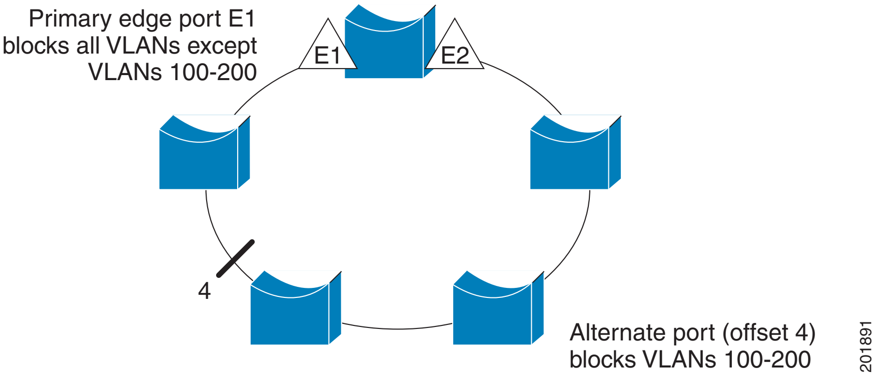
This example shows how to configure the same configuration when the interface has no external REP neighbor:

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet0/1
Switch (conf-if)# rep segment 1 edge no-neighbor primary
Switch (conf-if)# rep stcn segment 2-5
Switch (conf-if)# rep block port 0009001818D68700 vlan all
Switch (conf-if)# rep preempt delay 60
Switch (conf-if)# rep lsl-age-timer 6000
```

This example shows how to configure the VLAN blocking configuration shown in Figure 14-5. The alternate port is the neighbor with neighbor offset number 4. After manual preemption, VLANs 100 to 200 are blocked at this port, and all other VLANs are blocked at the primary edge port E1 (Gigabit Ethernet port 0/1).

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet0/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep block port 4 vlan 100-200
Switch (conf-if)# end
```

Figure 14-5 Example of VLAN Blocking



Setting Manual Preemption for VLAN Load Balancing

If you do not enter the **rep preempt delay** *seconds* interface configuration command on the primary edge port to configure a preemption time delay, the default is to manually trigger VLAN load balancing on the segment. Be sure to complete all other segment configuration before manually preempting VLAN load balancing. When you enter the **rep preempt segment** *segment-id* command, a confirmation message appears before the command is executed because preemption can cause network disruption.

Follow this procedure on the switch that has the segment primary edge port to manually trigger VLAN load balancing on a segment.

BEFORE YOU BEGIN

Configure REP interfaces as described in the "Configuring REP Interfaces" procedure on page 14-9.

DETAILED STEPS

	Command	Purpose
Step 1	**rep preempt segment** *segment-id*	Manually trigger VLAN load balancing on the segment. You need to confirm the command before it is executed.
Step 2	**show rep topology**	View REP topology information.

EXAMPLE

This example shows how to manually trigger REP preemption on segment 100 with the confirmation message:

```
Switch# rep preempt segment 100
The command will cause a momentary traffic disruption.
Do you still want to continue? [confirm]
```

Configuring SNMP Traps for REP

You can configure the switch to send REP-specific traps to notify the SNMP server of link operational status changes and port role changes.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp mib rep trap-rate** *value*	Enable the switch to send REP traps, and set the number of traps sent per second. The range is from 0 to 1000. The default is 0 (no limit imposed; a trap is sent at every occurrence).
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify the REP trap configuration.
Step 5	**copy running-config startup config**	(Optional) Save your entries in the switch startup configuration file.

To remove the trap, enter the **no snmp mib rep trap-rate** global configuration command.

EXAMPLE

This example configures the switch to send REP traps at a rate of 10 per second:

```
Switch(config)# snmp mib rep trap-rate 10
```

Verifying Configuration

Command	Purpose
show interface [*interface-id*] **rep** [**detail**]	Display REP configuration and status for a specified interface or for all interfaces.
show rep topology [**segment** *segment_id*] [**archive**] [**detail**]	Display REP topology information for a segment or for all segments, including the primary and secondary edge ports in the segment.

Configuration Example

This example shows how to configure the administrative VLAN as VLAN 100 and to verify the configuration by entering the **show interface rep detail** command on one of the REP interfaces:

```
Switch# configure terminal
Switch (conf)# rep admin vlan 100
Switch (conf-if)# end

Switch# show interface gigabitethernet0/1 rep detail
```

```
GigabitEthernet0/1 REP enabled
Segment-id: 2 (Edge)
PortID: 00010019E7144680
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 0002001121A2D5800E4D
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 100
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 3322, tx: 1722
HFL PDU rx: 32, tx: 5
BPA TLV rx: 16849, tx: 508
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 118, tx: 118
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 4214, tx: 4190
```

This example shows how to configure an interface as the primary edge port for segment 1, to send STCNs to segments 2 through 5, and to configure the alternate port as the port with port ID 0009001818D68700 to block all VLANs after a preemption delay of 60 seconds after a segment port failure and recovery. The interface is configured to remain up for 6000 milliseconds without receiving a hello from a neighbor.

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet0/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep stcn segment 2-5
Switch (conf-if)# rep block port 0009001818D68700 vlan all
Switch (conf-if)# rep preempt delay 60
Switch (conf-if)# rep lsl-age-timer 6000
Switch (conf-if)# end
```

This example shows how to configure the same configuration when the interface has no external REP neighbor:

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet0/1
Switch (conf-if)# rep segment 1 edge no-neighbor primary
Switch (conf-if)# rep stcn segment 2-5
Switch (conf-if)# rep block port 0009001818D68700 vlan all
Switch (conf-if)# rep preempt delay 60
Switch (conf-if)# rep lsl-age-timer 6000
```

This example shows how to configure the VLAN blocking configuration shown in Figure 14-5. The alternate port is the neighbor with neighbor offset number 4. After manual preemption, VLANs 100 to 200 are blocked at this port, and all other VLANs are blocked at the primary edge port E1 (Gigabit Ethernet port 0/1).

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet0/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep block port 4 vlan 100-200
Switch (conf-if)# end
```

This example shows how to manually trigger REP preemption on segment 100 with the confirmation message:

```
Switch# rep preempt segment 100
```

```
The command will cause a momentary traffic disruption.
Do you still want to continue? [confirm]
```

This example configures the switch to send REP traps at a rate of 10 per second:

```
Switch(config)# snmp mib rep trap-rate 10
```

Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS LAN Switching Command Reference

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520 Switch	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

Configuring UDLD

This chapter describes how to configure the UniDirectional Link Detection (UDLD) protocol on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*.

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 15-7.

This chapter includes the following sections:

Information About UDLD

UDLD is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. All connected devices must support UDLD for the protocol to successfully identify and disable unidirectional links. When UDLD detects a unidirectional link, it disables the affected port and alerts you. Unidirectional links can cause a variety of problems, including spanning-tree topology loops.

Modes of Operation

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD can detect unidirectional links due to misconnected ports on fiber-optic connections. In aggressive mode, UDLD can also detect unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and to misconnected ports on fiber-optic links.

In normal and aggressive modes, UDLD works with the Layer 1 mechanisms to learn the physical status of a link. At Layer 1, autonegotiation takes care of physical signaling and fault detection. UDLD performs tasks that autonegotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected ports. When you enable both autonegotiation and UDLD, the Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols.

A unidirectional link occurs whenever traffic sent by a local device is received by its neighbor but traffic from the neighbor is not received by the local device.

In normal mode, UDLD detects a unidirectional link when fiber strands in a fiber-optic port are misconnected and the Layer 1 mechanisms do not detect this misconnection. If the ports are connected correctly but the traffic is one way, UDLD does not detect the unidirectional link because the Layer 1 mechanism, which is supposed to detect this condition, does not do so. In this case, the logical link is considered undetermined, and UDLD does not disable the port.

When UDLD is in normal mode, if one of the fiber strands in a pair is disconnected, as long as autonegotiation is active, the link does not stay up because the Layer 1 mechanisms detects a physical problem with the link. In this case, UDLD does not take any action and the logical link is considered undetermined.

In aggressive mode, UDLD detects a unidirectional link by using the previous detection methods. UDLD in aggressive mode can also detect a unidirectional link on a point-to-point link on which no failure between the two devices is allowed. It can also detect a unidirectional link when one of these problems exists:

- On fiber-optic or twisted-pair links, one of the ports cannot send or receive traffic.
- On fiber-optic or twisted-pair links, one of the ports is down while the other is up.
- One of the fiber strands in the cable is disconnected.

In these cases, UDLD disables the affected port.

In a point-to-point link, UDLD hello packets can be considered as a heart beat whose presence guarantees the health of the link. Conversely, the loss of the heart beat means that the link must be shut down if it is not possible to re-establish a bidirectional link.

If both fiber strands in a cable are working normally from a Layer 1 perspective, UDLD in aggressive mode detects whether those fiber strands are connected correctly and whether traffic is flowing bidirectionally between the correct neighbors. This check cannot be performed by autonegotiation because autonegotiation operates at Layer 1.

Methods to Detect Unidirectional Links

UDLD operates by using two mechanisms:

- Neighbor database maintenance

  UDLD learns about other UDLD-capable neighbors by periodically sending a hello packet (also called an advertisement or probe) on every active port to keep each device informed about its neighbors.

  When the switch receives a hello message, it caches the information until the age time (hold time or time-to-live) expires. If the switch receives a new hello message before an older cache entry ages, the switch replaces the older entry with the new one.

Whenever a port is disabled and UDLD is running, whenever UDLD is disabled on a port, or whenever the switch is reset, UDLD clears all existing cache entries for the ports affected by the configuration change. UDLD sends at least one message to inform the neighbors to flush the part of their caches affected by the status change. The message is intended to keep the caches synchronized.

- Event-driven detection and echoing

  UDLD relies on echoing as its detection mechanism. Whenever a UDLD device learns about a new neighbor or receives a resynchronization request from an out-of-sync neighbor, it restarts the detection window on its side of the connection and sends echo messages in reply. Because this behavior is the same on all UDLD neighbors, the sender of the echoes expects to receive an echo in reply.

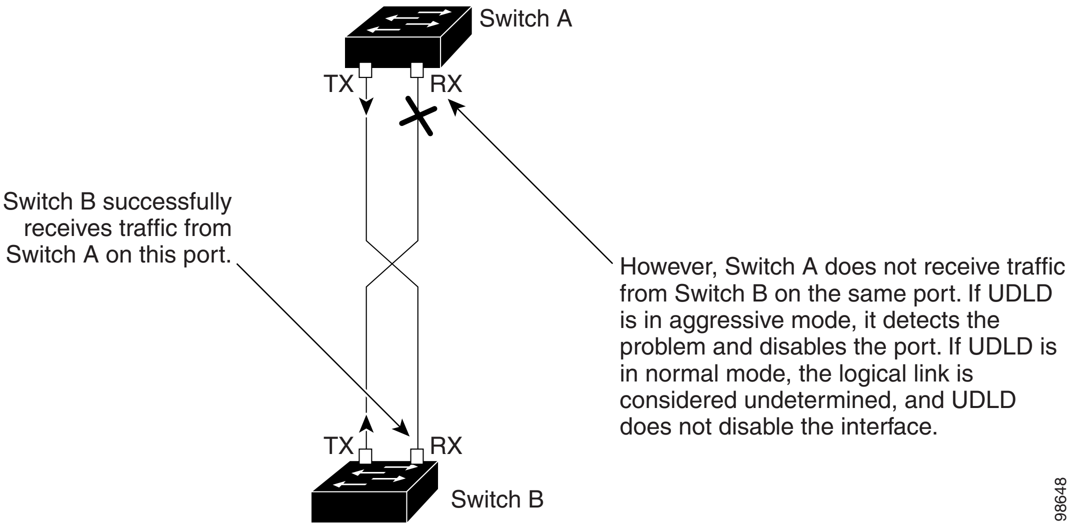
  If the detection window ends and no valid reply message is received, the link might shut down, depending on the UDLD mode. When UDLD is in normal mode, the link might be considered undetermined and might not be shut down. When UDLD is in aggressive mode, the link is considered unidirectional, and the port is disabled.

If UDLD in normal mode is in the advertisement or in the detection phase and all the neighbor cache entries are aged out, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbors.

If you enable aggressive mode when all the neighbors of a port have aged out either in the advertisement or in the detection phase, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbor. UDLD shuts down the port if, after the fast train of messages, the link state is still undetermined.

Figure 15-1 shows an example of a unidirectional link condition.

Figure 15-1 UDLD Detection of a Unidirectional Link


Switch A
TX
RX
Switch B successfully receives traffic from Switch A on this port.
However, Switch A does not receive traffic from Switch B on the same port. If UDLD is in aggressive mode, it detects the problem and disables the port. If UDLD is in normal mode, the logical link is considered undetermined, and UDLD does not disable the interface.
TX
RX
Switch B
98648

Guidelines and Limitations

- UDLD is not supported on ATM ports.
- A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch.

- When configuring the mode (normal or aggressive), make sure that the same mode is configured on both sides of the link.

Caution Loop guard works only on point-to-point links. We recommend that each end of the link has a directly connected device that is running STP.

Default Settings

Feature	Default Setting
UDLD global enable state	Globally disabled
UDLD per-port enable state for fiber-optic media	Disabled on all Ethernet fiber-optic ports
UDLD per-port enable state for twisted-pair (copper) media	Disabled on all Ethernet 10/100 and 1000BASE-TX ports
UDLD aggressive mode	Disabled

Configuring UDLD

- Enabling UDLD Globally, page 15-4
- Enabling UDLD on an Interface, page 15-5
- Resetting an Interface Disabled by UDLD, page 15-6

Enabling UDLD Globally

Follow this procedure to enable UDLD in the aggressive or normal mode and to set the configurable message timer on all fiber-optic ports on the switch.

BEFORE YOU BEGIN

Review the “Information About UDLD” section on page 15-1 and “Guidelines and Limitations” section on page 15-3.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**udld** {**aggressive** | **enable** | **message time** *message-timer-interval*}	Specify the UDLD mode of operation: • **aggressive**—Enables UDLD in aggressive mode on all fiber-optic ports. • **enable**—Enables UDLD in normal mode on all fiber-optic ports on the switch. UDLD is disabled by default. An individual interface configuration overrides the setting of the **udld enable** global configuration command. For more information about aggressive and normal modes, see the "Modes of Operation" section on page 15-1. • **message time** *message-timer-interval*—Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are detected to be bidirectional. The range is from 7 to 90 seconds. **Note** This command affects fiber-optic ports only. Use the **udld** interface configuration command to enable UDLD on other port types. For more information, see the "Enabling UDLD on an Interface" section on page 15-5.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show udld**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable UDLD globally, use the **no udld enable** global configuration command to disable normal mode UDLD on all fiber-optic ports. Use the **no udld aggressive** global configuration command to disable aggressive mode UDLD on all fiber-optic ports.

EXAMPLE

The following example shows how to enable UDLD in normal mode on all fiber interfaces:

```
Switch(config)# udld enable
```

Enabling UDLD on an Interface

Follow this procedure either to enable UDLD in the aggressive or normal mode or to disable UDLD on a port.

BEFORE YOU BEGIN

Review the "Information About UDLD" section on page 15-1 and "Guidelines and Limitations" section on page 15-3.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be enabled for UDLD, and enter interface configuration mode.
Step 3	**no shutdown**	Enable the port, if necessary. By default, user network interfaces (UNIs) and enhanced network interfaces (ENIs) are disabled, and network node interfaces (NNIs) are enabled.
Step 4	**udld port** [**aggressive**]	UDLD is disabled by default. • **udld port**—Enables UDLD in normal mode on the specified port. • **udld port aggressive**—Enables UDLD in aggressive mode on the specified port. **Note** Use the **no udld port** interface configuration command to disable UDLD on a specified fiber-optic port. For more information about aggressive and normal modes, see the "Modes of Operation" section on page 15-1.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show udld** *interface-id*	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

The following example shows how to cause a port interface to enable UDLD in the aggressive mode regardless of the current global **udld** (**aggressive** or **enable**) setting:

```
Switch(config-if)# udld port aggressive
```

Resetting an Interface Disabled by UDLD

Follow this procedure to reset all ports disabled by UDLD.

BEFORE YOU BEGIN

You can also bring up the port by using these commands:

- **The shutdown** interface configuration command followed by the **no shutdown** interface configuration command restarts the disabled port.
- The **no udld** {**aggressive | enable**} global configuration command followed by the **udld** {**aggressive | enable**} global configuration command re-enables the disabled ports.
- The **no udld port** interface configuration command followed by the **udld port** [**aggressive**] interface configuration command re-enables the disabled fiber-optic port.

- The **errdisable recovery cause udld** global configuration command enables the timer to automatically recover from the UDLD error-disabled state, and the **errdisable recovery interval** *interval* global configuration command specifies the time to recover from the UDLD error-disabled state.

DETAILED STEPS

	Command	Purpose
Step 1	**udld reset**	Reset all ports disabled by UDLD.
Step 2	**show udld**	Verify your entries.

EXAMPLE

This example shows how to reset all the ports that are error disabled by UDLD:

```
Switch# udld reset
```

Verifying Configuration

To display the UDLD status for the specified port or for all ports, use the **show udld** [*interface-id*] privileged EXEC command.

For detailed information about the fields in the command output, see the command reference listed in "Related Documents" section on page 15-7.

Configuration Example

The following example shows how to enable UDLD in normal mode on all fiber interfaces:

```
Switch(config)# udld enable
```

The following example shows how to cause a port interface to enable UDLD in the aggressive mode regardless of the current global **udld** (**aggressive** or **enable**) setting:

```
Switch(config-if)# udld port aggressive
```

This example shows how to reset all the ports that are error disabled by UDLD:

```
Switch# udld reset
```

Related Documents

Cisco IOS Master Command List, All Releases

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520 Switch	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

CHAPTER 16

Configuring Voice VLAN

This chapter describes how to configure Voice VLAN on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*.

Voice VLAN is referred to as an *auxiliary VLAN* in some Catalyst 6500 family switch documentation.

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 16-7.

This chapter includes the following sections:

Information About Voice VLAN

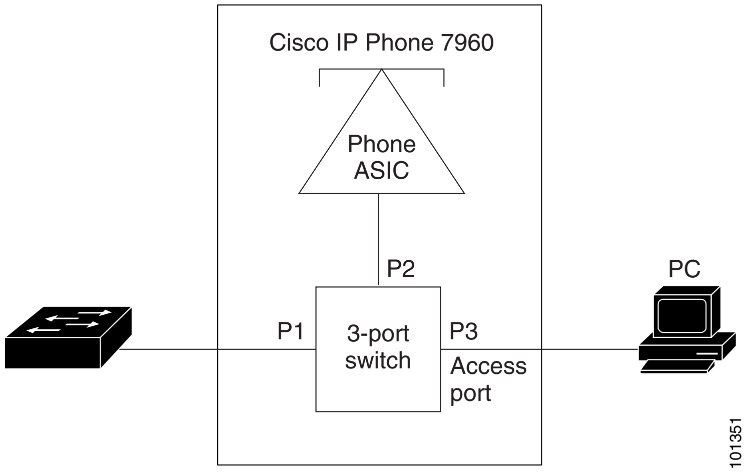
The Voice VLAN feature enables access ports to carry IP voice traffic from an IP phone.

When using a configurable IP phone, you can configure it to forward traffic with an IEEE 802.1p priority. You can also configure the switch to trust or override the traffic priority assigned by an IP phone. For example, a Cisco IP phone (such as 7960 series) contains an integrated three-port 10/100 switch as shown in Figure 16-1. The ports provide dedicated connections to these devices:

- Port 1 connects to the switch or other voice-over-IP (VoIP) device.
- Port 2 is an internal 10/100 interface that carries the IP Phone traffic.
- Port 3 (access port) connects to a PC or other device.

Figure 16-1 shows one way to connect a Cisco IP phone.

Figure 16-1 Cisco 7960 IP Phone Connected to a Switch



Cisco IP Phone Voice Traffic

You can configure an access port with an attached Cisco IP phone to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone. You can configure access ports on the switch to send Cisco Discovery Protocol (CDP) packets.

Cisco IP Phone Data Traffic

The switch can also process tagged data traffic (traffic in IEEE 802.1Q or IEEE 802.1p frame types) from the device attached to the access port on the Cisco IP phone (see Figure 16-1). You can configure Layer 2 access ports on the switch to send CDP packets that instruct the attached phone to configure the phone access in trusted mode. In this case, all traffic received through the access port on the Cisco IP phone passes through the phone unchanged.

Note Untagged traffic from the device attached to the Cisco IP phone passes through the phone unchanged, regardless of the trust state of the access port on the phone.

Prerequisites

- Be familiar with the information in the "Information About Voice VLAN" section on page 16-1 and "Guidelines and Limitations" section on page 16-3.
- Determine how you want the switch to process voice and data traffic.

Guidelines and Limitations

- Voice VLAN configuration is only supported on switch access ports; Voice VLAN configuration is not supported on trunk ports.

Note Trunk ports can carry any number of Voice VLANs, similar to regular VLANs. The configuration of Voice VLANs is not required on trunk ports.

  Voice VLAN should be present and active on the switch for the IP phone to correctly communicate on the Voice VLAN. Use the **show vlan** privileged EXEC command to display the configured VLANs.

- You must enable CDP on the switch port connected to the Cisco IP phone to send the configuration to the phone. (CDP is globally enabled by default on all switch interfaces.)
- The Port Fast feature is automatically enabled. When you configure Voice VLAN, the Port Fast feature is disabled by default.
- If the Cisco IP phone and a device attached to the phone are in the same VLAN, they must be in the same IP subnet. These conditions indicate that they are in the same VLAN:
  - They both use IEEE 802.1p or untagged frames.
  - The Cisco IP phone uses IEEE 802.1p frames, and the device uses untagged frames.
  - The Cisco IP phone uses untagged frames, and the device uses IEEE 802.1p frames.
  - The Cisco IP phone uses IEEE 802.1Q frames, and the Voice VLAN is the same as the access VLAN.
- The Cisco IP phone and a device attached to the phone cannot communicate if they are in the same VLAN and subnet but use different frame types because traffic in the same subnet is not routed (routing would eliminate the frame type difference).
- You cannot configure static secure MAC addresses in the Voice VLAN.
- Voice VLAN ports can also be these port types:
  - Dynamic access port. (See the "Configuring Dynamic-Access Ports on VMPS Clients" section on page 6-57.)
  - IEEE 802.1x authenticated port. (See the "Configuring 802.1x Readiness Check" section within the "Configuring IEEE 802.1x Port-Based Authentication" chapter of the *Security Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.

    Note If you enable IEEE 802.1x on an access port on which a Voice VLAN is configured and to which a Cisco IP phone is connected, the phone loses connectivity to the switch for up to 30 seconds.

  - Protected port. (See the Configuring Protected Ports section within the Configuring Port-Based Traffic Control chapter of the *System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.
  - A source or destination port for a SPAN or RSPAN session.
  - Secure port. (See the Configuring Port Security section within the Configuring Port-Based Traffic Control chapter of the *System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.

Note When you enable port security on an interface that is also configured with a Voice VLAN, you must set the maximum allowed secure addresses on the port to two plus the maximum number of secure addresses allowed on the access VLAN. When the port is connected to a Cisco IP phone, the phone requires up to two MAC addresses. The phone address is learned on the Voice VLAN and might also be learned on the access VLAN. Connecting a PC to the phone requires additional MAC addresses.

Default Settings

The Voice VLAN feature is disabled by default.

When the Voice VLAN feature is enabled, all untagged traffic is sent according to the default CoS priority of the port.

Configuring Voice VLAN

Because a Cisco IP phone also supports a connection to a PC or other device, a port connecting the switch to a Cisco IP phone can carry mixed traffic. You can configure a port to decide how the Cisco IP phone carries voice traffic and data traffic.

This section includes the following topics:

- Configuring Cisco IP Phone Voice Traffic, page 16-4
- Configuring the Priority of Incoming Data Frames, page 16-5

Configuring Cisco IP Phone Voice Traffic

You can configure a port connected to the Cisco IP phone to send CDP packets to the phone to configure the way in which the phone sends voice traffic. The phone can carry voice traffic in IEEE 802.1Q frames for a specified Voice VLAN with a Layer 2 CoS value. It can use IEEE 802.1p priority tagging to give voice traffic a higher priority and forward all voice traffic through the native (access) VLAN. The Cisco IP phone can also send untagged voice traffic or use its own configuration to send voice traffic in the access VLAN. In all configurations, the voice traffic carries a Layer 3 IP precedence value (the default is 5).

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 16-3.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface connected to the phone, and enter interface configuration mode.

	Command	Purpose
Step 3	**switchport voice vlan** {*vlan-id* | **dot1p** | **none** | **untagged**}}	Configure how the Cisco IP phone carries voice traffic: • *vlan-id*—Configure the phone to forward all voice traffic through the specified VLAN. By default, the Cisco IP phone forwards the voice traffic with an IEEE 802.1Q priority of 5. Valid VLAN IDs are 1 to 4094. • **dot1p**—Configure the phone to use IEEE 802.1p priority tagging for voice traffic and to use the default native VLAN (VLAN 0) to carry all traffic. By default, the Cisco IP phone forwards the voice traffic with an IEEE 802.1p priority of 5. • **none**—Allow the phone to use its own configuration to send untagged voice traffic. • **untagged**—Configure the phone to send untagged voice traffic.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interfaces** *interface-id* **switchport** or	Verify your Voice VLAN entries.
	show running-config interface *interface-id*	Verify your QoS and Voice VLAN entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the port to its default setting, use the **no switchport voice vlan** interface configuration command.

EXAMPLE

This example shows how to configure a port connected to a Cisco IP phone and how to use IEEE 802.1p priority tagging for voice traffic and use the default native VLAN (VLAN 0) to carry all traffic:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport voice vlan dot1p
Switch(config-if)# end
```

Configuring the Priority of Incoming Data Frames

You can connect a PC or other data device to a Cisco IP phone port. To process tagged data traffic (in IEEE 802.1Q or IEEE 802.1p frames), you can configure the switch to send CDP packets to instruct the phone how to send data packets from the device attached to the access port on the Cisco IP phone. You can configure the phone to not change (trust) or to override (not trust) the priority of frames arriving on the phone port from connected devices.

BEFORE YOU BEGIN

To set priority of incoming data frames, the switch must be running the LAN Base image.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface connected to the Cisco IP phone, and enter interface configuration mode.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show interfaces** *interface-id* **switchport**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Verifying Configuration

Command	Purpose
show interfaces *interface-id* **switchport**	Display Voice VLAN configuration for an interface

Configuration Example

This example shows how to configure a port connected to a Cisco IP phone and how to use IEEE 802.1p priority tagging for voice traffic, and to use the default native VLAN (VLAN 0) to carry all traffic:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport voice vlan dot1p
Switch(config-if)# end
```

This example shows how to configure a port connected to a Cisco IP phone to not change the priority of frames received from the PC or the attached device:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# end
```

To return the port to its default setting, use the **no switchport priority extend** interface configuration command.

Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS Interface and Hardware Component Command Reference
- Security Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches
- System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520 Switch	Cisco IOS Release 15.0(2)ED
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 15.0(2)ED