show vlan through spanning-tree vlan

show vlan

To display VLAN information, use the **show vlan** command in privileged EXEC mode.

show **vlan** [{**all** | **brief** | **id** *vlan-id* | **name** *name* [**ifindex**] | **ifindex**}]

Syntax Description

all	(Optional) Displays all VLAN information.
brief	(Optional) Displays only a single line for each VLAN, naming the VLAN, status, and ports.
id *vlan-id*	(Optional) Displays information about a single VLAN that is identified by a VLAN ID number; valid values are from 1 to 4094.
name *name*	(Optional) Displays information about a single VLAN that is identified by VLAN name; valid values are an ASCII string fro m 1 to 32 char acters.
ifindex	(Optional) Displays the VLAN's ifIndex number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Each Ethernet switch port and Ethernet repeater group belong to only one VLAN. Trunk ports can be on multiple VLANs.

If you shut down a VLAN using the **state suspend** or the **state active**command, these values appear in the Status field:

- suspended--VLAN is suspended.
- active--VLAN is active.

If you shut down a VLAN using the **shutdown** command, these values appear in the Status field:

- act/lshut--VLAN status is active but shut down locally.
- sus/lshut--VLAN status is suspended but shut down locally.

This is an example of the output for a VLAN (VLAN0002) that is active but shut down locally:

```
Router# show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa5/9
2    VLAN0002                         act/lshut Fa5/9
<...Output truncated...>
```

If a VLAN is shut down internally, these values appear in the Status field:

- act/ishut--VLAN status is active but shut down internally.
- sus/ishut--VLAN status is suspended but shut down internally.

This is an example of the output for a VLAN (VLAN0002) that is active but shut down internally:

```
Router# show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa5/9
2    VLAN0002                         act/ishut Fa5/9
<...Output truncated...>
```

If a VLAN is shut down locally and internally, the value that is displayed in the Status field is act/ishut or sus/ishut. If a VLAN is shut down locally only, the value that is displayed in the Status field is act/lshut or sus/lshut.

Separate VLAN ranges with a hyphen, and separate VLANs with a comma and no spaces in between. For example, you can enter the following:

```
Router# show vlan id 1-4,3,7,5-20
```

When displaying a single VLAN both trunk and non-trunk ports are displayed. A non-trunk port is a port that is not configured as pm_port_mode_trunk. If an interface is configured as “switchport port mode trunk” it is displayed whether the link is up or down.

When displaying multiple VLANs only non-trunk ports are displayed.

Examples

This example shows how to display the VLAN parameters for all VLANs within the administrative domain:

```
Router# show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa5/9
2    VLAN0002                         active    Fa5/9
3    VLAN0003                         active    Fa5/9
4    VLAN0004                         active    Fa5/9
5    VLAN0005                         active    Fa5/9
6    VLAN0006                         active    Fa5/9
<...Output truncated...>

1004 fddinet-default                  active    Fa5/9
1005 trbrf-default                    active    Fa5/9

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        303    0
4    enet  100004     1500  -      -      -        -    -        304    0
5    enet  100005     1500  -      -      -        -    -        305    0
6    enet  100006     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
<...Output truncated...>

Remote SPAN VLANs
```

```
-----------------
2, 20
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
Router#
```

This example shows how to display the VLAN name, status, and associated ports only:

```
Router# show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa5/9
2    VLAN0002                         active    Fa5/9
3    VLAN0003
act/lshut
 Fa5/9
4    VLAN0004
act/lshut
 Fa5/9
5    VLAN0005                         active    Fa5/9
10   VLAN0010                         active    Fa5/9
.
.
.
999  VLAN0999                         active    Fa5/9
1002 fddi-default                     active    Fa5/9
1003 trcrf-default                    active    Fa5/9
1004 fddinet-default                  active    Fa5/9
1005 trbrf-default                    active    Fa5/9
Router#
```

This example shows how to display the VLAN parameters for multiple VLANs:

```
Router# show vlan id 1-4,3,7,5-20
VLAN Name                             Status    Ports
---- -------------------------------- --------- ------------------------------
1    default                          active    Fa5/7, Fa5/12
2    VLAN0002                         active
3    VLAN0003                         act/lshut
4    VLAN0004                         act/lshut
5    VLAN0005                         active
6    VLAN0006                         active
10   VLAN0010                         active
20   VLAN0020                         active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        303    0
4    enet  100004     1500  -      -      -        -    -        304    0
5    enet  100005     1500  -      -      -        -    -        305    0
6    enet  100006     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

Router#
```

This example shows how to display the ifIndex number for VLAN 10 only:

```
Router# show vlan id 10 ifindex

 VLAN Ifindex
 ---- -------
 10   37
Router#
```

The table below describes the fields that are shown in the example.

Table 1: show vlan Command Output Fields

Field	Description
VLAN	VLAN number.
Name	Name, if configured, of the VLAN.
Status	Status of the VLAN (active or suspend, act/lshut or sus/lshut, or act/ishut or sus/ishut).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.
BrdgNo	Bridge number for the VLAN, if applicable.
Stp	Spanning Tree Protocol type that is used on the VLAN.
BrdgMode	Bridging mode for this VLAN--possible values are SRB and SRT; the default is SRB.
AREHops	Maximum number of hops for All-Routes Explorer frames--possible values are 1 through 13; the default is 7.
STEHops	Maximum number of hops for Spanning Tree Explorer frames--possible values are 1 through 13; the default is 7.
Backup CRF	Status of whether the TrCRF is a backup path for traffic.
Ifindex	Number of the ifIndex.
Remote SPAN VLAN	RSPAN status.
Primary	Number of the primary VLAN.
Secondary	Number of the secondary VLAN.
Ports	Indicates the ports within a VLAN.

Field	Description
Type	Type of VLAN--Possible values are primary, isolated, community, nonoperation, or normal.

Related Commands

Command	Description
show vlan private-vlan	Displays PVLAN information.
vlan (config-VLAN submode)	Configures a specific VLAN.
vtp	Configures the global VTP state.

show vlan access-log config

To display VLAN access control list (VACL) logging configuration properties, use the **showvlanaccess-logconfig**command in privileged EXEC mode.

show vlan access-log config

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Syslog messages are generated when the device reaches the set threshold, or five minutes after the previous message is displayed, whichever occurs first. The threshold controls the rate of the syslog message only and does not affect the log table entries. Packets exceeding the specified rate limit will not be logged.

Examples

The following example shows how to display the configured VACL logging properties. The fields are self-explanatory.

```
Router# show vlan access-log config
VACL Logging Configuration:
        max log table size     :500
        log threshold          :4000
        rate limiter           :3000
```

Related Commands

Command	Description
show vlan access-log flow	Displays the contents of the VACL flow table.
show vlan access-log statistics	Displays packets, message counts, and other statistics of the VACL.
vlan access-log	Configures VACL logging properties, including the log-table size, redirect-packet rate, and logging threshold.

show vlan access-log flow

To display VLAN access control list (VACL) flow table contents, use the **showvlanaccess-logflow**command in privileged EXEC mode.

show vlan access-log flow *protocol* {*src-addr src-mask* | **any** | **host** {*hostnamehost-ip*}} {*dst-addr dst-mask* | **any** | **host** {*hostnamehost-ip*}} [**vlan** *vlan-id*]

Syntax Description

protocol	Protocol name or number; valid values are **icmp**, **igmp**, **ip**, **tcp**, **udp**, or numbers from 0 to 255 to designate a protocol.
src-addr src-mask	Source address and mask.
any	Displays information for any host.
host *hostname*	Displays information for a hostname.
host *host-ip*	Displays information for a host IP address.
dst-addr dst-mask	Destination address and mask.
vlan *vlan-id*	(Optional) Displays information for a specific VLAN valid value. Range is from 1 to 4094.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Entries for the standard protocols or any protocol can be displayed by specifying the protocol name or protocol number. Entries are removed from the table, if there is no increment in the packet counter after the last syslog message.

Examples

The following example shows how to display the VACL flow table contents.

```
Router# show vlan access-log flow 17 172.20.10.110 255.255.0.0 172.20.10.105
 255.255.0.0
id  prot    src_ip         dst_ip      sport  dport vlan    port    count   total    lastlog
-------------------------------------------------------------------------------------
1  17   172.20.10.110   172.20.10.105    68     67    2    Gi1/0/3    324     325  00:03:14.338
2  17   172.20.10.109   172.20.10.105    68     67    2    Gi1/0/3    324     325  00:03:13.843
3  17   172.20.10.108   172.20.10.105    68     67    2    Gi1/0/3    325     326  00:03:13.340
4  17   172.20.10.107   172.20.10.105    68     67    2    Gi1/0/3    326     327  00:03:12.845
5  17   172.20.10.106   172.20.10.105    68     67    2    Gi1/0/3    327     328  00:03:12.342
6  17   172.20.10.110   172.20.10.105    68     67    2    Gi1/0/2    603     604  00:02:32.202
```

```
7  17   172.20.10.109   172.20.10.105    68    67   2    Gi1/0/2    605    606  00:02:31.204
8  17   172.20.10.108   172.20.10.105    68    67   2    Gi1/0/2    607    608  00:02:30.206
9  17   172.20.10.107   172.20.10.105    68    67   2    Gi1/0/2    607    608  00:02:29.216
10  17   172.20.10.106   172.20.10.105    68    67  2    Gi1/0/2    607    608  00:02:28.201
Total number of matched entries: 10
```

The table below describes the significant fields shown in the display.

Table 2: show vlan access-log flow Field Descriptions

Field	Description
prot	Protocol number.
src_ip	Source IP address.
dst_ip	Destination IP address.
sport	Source port.
dport	Destination port.
vlan	VLAN on which the packet arrived.
port	Physical interface on which the packet arrived.
count	Indicates the number of packets generated since the last syslog message was generated.
total	Cumulative count of packets for the flow.
lastlog	Time stamp of the last log.

Related Commands

Command	Description
show vlan access-log config	Displays VACL logging configuration properties.
show vlan access-log statistics	Displays packets, message counts, and other statistics of the VACL.
vlan access-log	Configures VACL logging properties, including the log-table size, redirect-packet rate, and logging threshold.

show vlan access-log statistics

To display VLAN access control list (VACL) packet counts, messages, and other statistics, use the **showvlanaccess-logstatistics**command in privileged EXEC mode.

show vlan access-log statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

All platforms do not display VACL logging index. Packets that are dropped do not generate any syslog messages.

Examples

The following example shows how to display the VACL statistics. The fields are self-explanatory.

```
Router# show vlan access-log statistics
VACL Logging Statistics:
        total packets          :0
        logged                 :0
        dropped                :0
Dropped Packets Statistics:
        unsupported protocol   :0
        no packet buffer       :0
        hash queue full        :0
        flow table full        :0
Misc Information:
        VACL Logging LTL Index :0x7E02
        free packet buffers    :8192
        log messages sent      :0
        log table size         :0
```

Related Commands

Command	Description
show vlan access-log config	Displays VACL logging configuration properties.
show vlan access-log flow	Displays the contents of the VACL flow table.
vlan access-log	Configures VACL logging properties, including the log-table size, redirect-packet rate, and logging threshold.

show vlan access-map

To display the contents of a VLAN-access map, use the **showvlanaccess-map** command in privileged EXEC mode.

show vlan access-map [*map-name*]

Syntax Description

map-name	(Optional) VLAN access-map name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1.(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.

Examples

The following example shows how to display the contents of a VLAN-access map. The fields shown in the display are self-explanatory.

```
Device# show vlan access-map access-map-example-1

Vlan access-map access-map-example-1
        match: ip address 13
        action: forward capture
```

```
Device# show vlan access-map vl10

match clauses:
 ipv6 address: v6acl
Action:
 drop
```

Related Commands

Command	Description
action	Sets the packet action clause.
match	Specifies the match clause by selecting one or more ACLs for a VLAN access-map sequence.
vlan access-map	Creates a VLAN access map or enters VLAN access-map command mode.

show vlan all-ports

To display VLAN information for trunk and access ports, use the**showvlanall-ports** command in privileged EXEC mode.

show vlan all-ports

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Examples

The following example shows how to display VLAN information for trunk and access ports:

```
Router# show vlan all-ports
VLAN Name Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
2    VLAN0002                         active
3    VLAN0003                         active
.
.
.
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                      act/unsup
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        303    0
.
.
.
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 trcrf 101003     4472  1005   3276   -        -    srb      0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trbrf 101005     4472  -      -      15       ibm  -        0      0
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1005 trbrf 101005     4472  -      -      15       ibm  -        0      0
VLAN AREHops STEHops Backup CRF
---- ------- ------- ----------
802  0       0       off
1003 7       7       off
Primary Secondary Type            Ports
------- --------- ----------------- ------------------------------------------
```

The table below describes the significant fields shown in the display.

Table 3: show vlan all-ports Field Descriptions

Field	Description
VLAN	VLAN number.
Name	Name, if configured, of the VLAN.
Status	Status of the VLAN (active or suspend).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.
BridgeNo	Bridge number for the VLAN, if applicable.
Stp	Spanning-Tree Protocol type used on the VLAN.
BrdgMode	Bridging mode for this VLAN--Possible values are source-route bridging (SRB) and source-route transparent bridging (SRT); the default is SRB.
Trans1, Trans2	Types of translational bridges that the VLAN in the VLAN column is configured to translate to. Translational bridge VLANs must be a VLAN media type different from the affected VLAN; if two VLANs are specified, each one must be a different type. Common VLAN types include Ethernet (enet), FDDI (fdnet), and Token Ring (tnet). The numbers in the "Trans1" and "Trans2" columns refer to the VLAN ID numbers of the translational bridge VLANs. **Note** The term "VLAN translation" is also used in Cisco configuration guides for mapping specific VLANs in a given trunk to another VLAN that is of the same media type. In this context the term "VLAN translation" refers to a form of VLAN mapping that is using the term "VLAN translation" to describe it.
AREHops	Number of All Route Explorer (ARE) hops.
STEHops	Number of Spanning-Tree Explorer (STE) hops.
Backup CRF	Status of the backup Concentrator relay function (CRF).
primary	Primary VLAN.
secondary	Secondary VLAN.

show vlan counters

To display the software-cached counter values, use the **showvlancounters** command in privileged EXEC mode.

show vlan [**id** *vlanid*] **counters**

Syntax Description

id *vlanid*	(Optional) Displays the software-cached counter values for a specific VLAN; valid values are from 1 to 4094.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was introduced.
12.2(50)SY	This command was introduced. Command output was updated to count broadcast packets with Unicast counters.

Usage Guidelines

The **showvlanidcounters** command is not supported on switch virtual interfaces (SVIs).

For Layer 2 and Layer 3 VLAN interfaces and router ports, per-interface switching statistics and VLAN-counter information to the Multilayer Switching Feature Card 2 (MSFC2) are exported approximately every 3 minutes.

If you enter the **showvlancounters** command with no arguments, the software-cached counter values for all VLANs are displayed.

Examples

This example shows how to display the software-cached counter values for a specific VLAN. The fields shown in the display are self-explanatory.

```
Router# show vlan id 205 counters
VLAN vlanid 205
L2-Unicast-Pkts      10
L3-In-Unicast-Pkts   0
L3-Out-Unicast-Pkts  0
L2-NonUnicast-Pkts + L3-In-NonUnicast-Pkts  5
L3-Out-NonUnicast-Pkts   6
L2-Unicast-Octets 6
L3-In-Unicast-Octets 6
L3-Out-Unicast-Octets 6
L2-NonUnicast-Octets + L3-In-NonUnicast-Octets 6
L3-Out-NonUnicast-Octets 6
Router#
```

Related Commands

Command	Description
clear vlan counters	Clears the software-cached counter values to zero for a specified VLAN or all existing VLANs.

show vlan dot1q tag native

To display native VLAN-tagging information, use the **showvlandot1qtagnative** command in privileged EXEC mode.

show vlan dot1q tag native

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display native VLAN-tagging information. The fields shown in the display are self-explanatory.

```
Router# show vlan dot1q tag native
dot1q native vlan tagging is enabled
Internal dot1q native vlan: 1015
Router#
```

Related Commands

Command	Description
vlan dot1q tag native	Enables dot1q tagging for all VLANs in a trunk.

show vlan filter

To display information about the VLAN filter, use the **showvlanfilter** command in privileged EXEC mode.

show vlan filter [{**access-map** *map-name* | **vlan** *vlan-id* | **interface** *interface interface-number*}]

Syntax Description

access-map *map-name*	(Optional) Displays the VLANs that are filtered by the specified map.
vlan *vlan-id*	(Optional) Displays the filter for the specified VLAN; valid values are from 1 to 4094.
interface *interface*	(Optional) Specifies the interface type; valid values are **pos**, **atm**, or **serial**. See the "Usage Guidelines" section for additional information.
interface-number	(Optional) Interface number; see the "Usage Guidelines" section for additional information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **showvlanfilter***map-name***interface** command accepts only ATM, packet over SONET/SDH (POS), or serial interface types. If your system is not configured with any of these interface types, the **interface***interfaceinterface-number* keyword and arguments are not provided.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 2 to 13 and valid values for the port number are from 1 to 48.

If you do not specify an optional keyword and argument, all mappings are displayed. If you enter access-map *map_name*, all the VLANs and interfaces that are associated with the specified map are shown. If you enter vlan *vlan-id* or **interface***interfaceinterface-number*, its associated access map, if existing, is shown.

In the output for VLAN access control lists (VACLs) on VLANs, the following applies:

- Configured on VLANs--User configured
- Active on VLANs--VLAN list on which the VACL is active

In the WAN-interface outputs, the following applies:

- Configured on interfaces--User configured
- Active on Interfaces--Interfaces on which the VACL is active

Examples

This example shows how to display mappings between the VACLs and the VLANs and the VACLs and the interfaces. The fields shown in the display are self-explanatory.

```
Router# show vlan filter
VLAN Map mordred:
   Configured on VLANs: 2,4-6
   Active on VLANs: 2,4-6
Router#
```

Related Commands

Command	Description
vlan access-map	Creates a VLAN access map or enters VLAN access-map command mode.
vlan filter	Applies a VLAN access map.

show vlan free

To display the total number of free VLANs on a router, use the show vlan free command in privileged EXEC mode .

show vlan free

Syntax Description

This command has no arguments or keywords.

Command Default

All free VLANs are displayed.

Command Modes

Privileged EXEC (#)

Usage Guidelines

The**showvlanfree** command displays the total number of free VLANs on a router.

Command History

Release	Modification
12.2(33)SRE	This command was introduced on the Cisco 7600 series routers.

Examples

The following is sample output from the **showvlanfree** command. This example lists the number of free VLANs on a router. The fields shown in the display are self-explanatory.

```
Router#
show vlan free
Free VLANs
----------
2
3
4
5
6
7
8
9
10
```

Related Commands

Command	Description
show vlan	Displays the VLAN information in the system.

show vlan free summary

To display the usage summary of all the free VLANs in the system, use the **show free vlan summary** command in privileged EXEC mode.

show vlan free summary

Syntax Description

This command has no arguments or keywords.

Command Default

Summary information for all the internal free VLANs is displayed.

Command Modes

Privileged EXEC (#)

Usage Guidelines

The **show vlan free summary** command displays the following VLAN information:

- Total number of available VLANs
- Total number of free VLANs
- Total number of used VLANs

Command History

Release	Modification
12.2(33)SRE	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to view the summary information for the existing VLANs in the system. The field descriptions shown in the display are self-explanatory.

```
Device# show vlan free summary

======= vlan free/usage Summary =======
Total number of available vlans = 4094
Total number of free vlans = 4074
Total number of used vlans = 20
```

Related Commands

Command	Description
show vlan free	Displays the total number of the free VLANs on a router.

show vlan internal free summary

To display the summary information of all the internal free VLANs, use the **show vlan internal free summary** command in privileged EXEC mode.

show vlan internal free summary

Syntax Description

This command has no arguments or keywords.

Command Default

Summary information for all the internal free VLANs is displayed.

Command Modes

Privileged EXEC (#)

Usage Guidelines

The **show vlan internal free summary** command displays the following VLAN information:

- Total number of available internal VLANs
- Total number of free internal VLANs
- Total number of used internal VLANs

Command History

Release	Modification
15.4(2)S	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to view the summary information for all the free internal VLANs in the system. The field descriptions shown in the display are self-explanatory.

```
Device# show vlan internal free summary

======= vlan free/usage Summary =======
Total number of available vlans = 4094
Total number of free vlans = 4078
Total number of used vlans = 16
```

Related Commands

Command	Description
show vlan free	Displays the total number of the free internal VLANs on a device.
show vlan free summary	Displays the usage summary of the free internal VLANs on a device.

show vlan internal usage

To display information about the internal VLAN allocation, use the **showvlaninternalusage** command in privileged EXEC mode.

show vlan [**id** *vlan-id*] **internal usage**

Syntax Description

id *vlan-id*	(Optional) Displays information about the internal VLAN allocation for the specified VLAN; valid values are from 1 to 4094.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

In some cases, the output displays the following:

```
workaround vlan
```

A workaround VLAN is used to enable the Policy Feature Card (PFC)-based policing on the PWAN1 main interface. Without the workaround VLAN, the packets hit the PFC policer twice for PWAN1 because the same VLAN is used when packets traverse the local bus before and after Parallel eXpress Forwarding (PXF) processing.

Entering the **showvlaninternalusage** command displays the Optical Services Module (OSM) interfaces and subinterfaces in addition to the regular Ethernet interfaces.

To display the associated subinterfaces, enter the **showcwanvlan** command. The **showcwanvlan** command displays the mapping between the WAN subinterface and the internal VLANs in use.

Examples

This example shows how to display the current internal VLAN allocation. The fields shown in the displays are self-explanatory.

```
Router# show vlan internal usage

VLAN Usage
---- --------------------
1025 -
1026 -
1027 -
1028 -
1029 Port-channel6
1030 GigabitEthernet1/2
1032 FastEthernet3/20
1033 FastEthernet3/21
1129 -
```

This example shows how to display the internal VLAN allocation for a specific VLAN:

```
Router# show vlan id 1030 internal usage
VLAN Usage
---- --------------------
1030 GigabitEthernet1/2
```

show vlan mapping

To register a mapping of an 802.1Q VLAN to an Inter-Switch Link (ISL) VLAN, use the **showvlanmapping** command in privileged EXEC mode.

show vlan mapping

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to list the map for an 802.1Q VLAN to an ISL VLAN. The fields shown in the display are self-explanatory.

```
Router# show vlan mapping
802.1Q Trunk Remapped VLANs:
802.1Q VLAN ISL VLAN
----------- -----------
101         202
200         330
Router#
```

Related Commands

Command	Description
show interfaces vlan mapping	Displays the status of a VLAN mapping on a port.
switchport vlan mapping enable	Enables VLAN mapping per switch port.

show vlan port provisioning

To display the VLAN port provisioning status, use the **showvlanportprovisioning**command in privileged EXEC mode.

show vlan port provisioning

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Examples

The following example shows how to display the VLAN port provisioning status. The fields shown in the display are self-explanatory.

```
Router# show vlan port provisioning
port provision: disabled
```

Related Commands

Command	Description
vlan port provisioning	Enables or disables VLAN port provisioning.

show vlan private-vlan

To display private VLAN (PVLAN) information, use the **show** vlan private-vlan command in privileged EXEC mode.

show vlan private-vlan [**type**]

Syntax Description

type	(Optional) Displays the PVLAN type (isolated, community, or primary).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

In the **showvlanprivate-vlantype** command output display, “normal” displayed as a type indicates a regular VLAN that is configured in a PVLAN. A display of “normal” means that two VLANs have been associated before the type was set and that the PVLAN is not operational. This information is useful for debugging purposes.

Examples

This example shows how to display information about all currently configured PVLANs:

```
Router#
show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
2       301       community         Fa5/3, Fa5/25
2       302       community
        10        community
100     101       isolated
150     151       non-operational
        202       community
        303       community
401     402       non-operational
Router#
```

This example shows how to display information about all currently configured PVLAN types:

```
Router#
show vlan private-vlan
 type
Vlan Type
---- -----------------
202  primary
303  community
304  community
305  community
306  community
307  community
```

```
308  normal
309  community
440  isolated
Router#
```

The table below describes the fields that are shown in the example.

Table 4: show vlan private-vlan Command Output Fields

Field	Description
Primary	Number of the primary VLAN.
Secondary	Number of the secondary VLAN.
Secondary-Type	Secondary VLAN type--Possible values are isolated or community.
Ports	Indicates the ports within a VLAN.
Type	Type of VLAN--Possible values are primary, isolated, community, nonoperation, or normal.

Related Commands

Command	Description
private-vlan mapping	Creates a mapping between the primary and the secondary VLANs so that both VLANs share the same primary VLAN SVI.
private-vlan	Configures PVLANs and the association between a PVLAN and a secondary VLAN.

show vlan remote-span

To display a list of remote Switched Port Analyzer (RSPAN) VLANs, use the **showvlanremote-span**command in privileged EXEC mode.

show vlan remote-span

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display a list of remote SPAN VLANs. The fields shown in the display are self-explanatory.

```
Router#
show vlan remote-span
Remote SPAN VLANs
------------------------------------------------------------------------------
2,20
```

Related Commands

Command	Description
remote-span	Configures a VLAN as an RSPAN VLAN.
vlan (config-VLAN submode)	Configures a specific VLAN.

show vlan virtual-port

To display the number of logical virtual ports required, use the **show** vlan virtual-port command in privileged EXEC mode.

show vlan virtual-port [**slot** *number*]

Syntax Description

slot *number*	(Optional) Specifies the slot number of which status is to be displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display the number of logical virtual ports that are required for a specific slot. The fields shown in the display are self-explanatory.

```
Router#
show vlan virtual-port slot 3
Slot 3
Port        Virtual-ports
-------------------------
Fa3/1             1
Fa3/2             1
Fa3/3             1
Fa3/4             1
Fa3/5             1
Fa3/6             1
Fa3/7             1
Fa3/8             1
Fa3/11            1
Fa3/12            1
Fa3/13            1
.
.
.
Fa3/33            4
Fa3/34            4
Fa3/35            4
Fa3/36            4
Fa3/37            4
Fa3/38            4
Fa3/39            4
Fa3/40            4
Total virtual ports:82
Router#
```

This example shows how to display the number of logical virtual ports that are required for all slots. The fields shown in the display are self-explanatory.

```
Router#
show vlan virtual-port
Slot 1
-------
Total slot virtual ports 1
Slot 3
-------
Total slot virtual ports 82
Slot 4
-------
Total slot virtual ports 4
Total chassis virtual ports 87
Router#
```

show vlan-range

To display the VLAN range, use the **showvlan-range** command in privileged EXEC mode.

show vlan-range

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.1	This command was modified. This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following is sample output from the **showvlan-range** command. The field descriptions in the display are self-explanatory.

```
Router# show vlan-range
IDB-less VLAN Ranges on FastEthernet0/1 (1 ranges)
7-67                                    (range)
```

Related Commands

Command	Description
vlan-range dot1q	Enables IEEE 802.1Q VLAN encapsulation for a range of VLANs on Ethernet interface.

show vlans dot1q

To display statistics about 802.1Q VLAN subinterfaces, use the **showvlansdot1q** command in privileged EXEC mode.

show vlans dot1q [{**internal** | *interface-type interface-number* **.** *subinterface-number* [**detail**] | *outer-id* [{*interface-type interface-number* | **second-dot1q** [{*inner-id* | **any**}]}] [**detail**]}]

Syntax Description

internal	(Optional) Displays internal QinQ VLAN tag termination information. Used for troubleshooting purposes. The QinQ VLAN Tag Termination feature on the subinterface level preserves VLAN IDs and keeps traffic in different customer VLANs segregated.
interface-type	(Optional) Interface type.
interface-number	(Optional) Interface number.
. *subinterface-number*	(Optional) Subinterface number in the range 1 to 4294967293. A period (**.**) must be entered between the *interface-number* argument and the *subinterface-number* argument.
detail	(Optional) Displays detailed information.
outer-id	(Optional) Outer VLAN identifier. The allowed range is from 1 to 4095.
second-dot1q	(Optional) Displays inner VLAN subinterface information.
inner-id	(Optional) Inner VLAN identifier. The allowed range is from 1 to 4095.
any	(Optional) Displays information for all the inner VLAN subinterfaces configured as "any." **Note** The any keyword is not supported on a subinterface configured for IPoQinQ because IP routing is not supported on ambiguous subinterfaces.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(7)XI7	This command was integrated into Cisco IOS Release 12.3(7)XI7 and implemented on the Cisco 10000 series routers.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines

If no arguments or keywords are entered, statistics for all of the 802.1Q VLAN IDs are displayed.

The any keyword is not supported for IPoQinQ because IP routing is not supported on ambiguous subinterfaces. However, the second-dot1q inner-id keyword and argument can be used on IPoQinQ for a specific inner VLAN ID that is not an ambiguous subinterface.

Note On the Cisco 10000 series router, the following is an implementation limitation--when a service policy is applied to a PPPoEoQinQ or IPoQinQ subinterface and the service policy drops some packets, the packets dropped are still displayed in the outgoing packet counters as output.

Note For the Cisco ASR 1000 Series Aggregation Services Router only, the command output includes the total number of packets dropped from the shared port adapter (SPA) because of ingress oversubscription on the VLAN. An example of the output is included in the section below.

Examples

802.1Q VLAN Statistics: Example

The output from the **showvlansdot1q**command displays the statistics for all the 802.1Q VLAN IDs. Only the outer VLAN IDs are displayed here.

```
Router# show vlans dot1q
Total statistics for 802.1Q VLAN 1:
   441 packets, 85825 bytes input
   1028 packets, 69082 bytes output
Total statistics for 802.1Q VLAN 101:
   5173 packets, 510384 bytes input
   3042 packets, 369567 bytes output
Total statistics for 802.1Q VLAN 201:
   1012 packets, 119254 bytes input
   1018 packets, 120393 bytes output
Total statistics for 802.1Q VLAN 301:
   3163 packets, 265272 bytes input
   1011 packets, 120750 bytes output
Total statistics for 802.1Q VLAN 401:
   1012 packets, 119254 bytes input
   1010 packets, 119108 bytes output
```

The table below describes the significant fields shown in the display.

Table 5: show vlans dot1q Field Descriptions

Field	Description
Total statistics for 802.1Q VLAN 1	Statistics are shown for the VLAN ID with the specified outer ID.
packets	Number of packets encapsulated by the 802.1Q QinQ VLAN.
bytes input	Number of bytes input.
bytes output	Number of bytes output.

The following sample output from the **showvlansdot1q**command displays the statistics for the 802.1Q VLAN subinterface configured on Gigabit Ethernet interface 5/0:

```
Router# show vlans dot1q GigabitEthernet 5/0.1011001
GigabitEthernet5/0.1011001 (101/1001)
   1005 packets, 122556 bytes input
   1023 packets, 125136 bytes output
```

The table below describes the significant fields shown in the display.

Table 6: show vlans dot1q (subinterface) Field Descriptions

Field	Description
GigabitEthernet5/0.1011001 (101/1001)	Statistics are shown for subinterface Gigabit Ethernet 5/0.1011001 with an outer VLAN ID of 101 and an inner VLAN ID of 1001.
packets	Number of packets encapsulated by the 802.1Q QinQ VLAN.
bytes input	Number of bytes input.
bytes output	Number of bytes output.

The following sample output from the **showvlansdot1q**command displays the summary statistics for all of the VLAN subinterfaces under the physical interface Gigabit Ethernet 5/0 that have an outer VLAN ID of 101:

```
Router# show vlans dot1q 101 GigabitEthernet 5/0
Total statistics for 802.1Q VLAN 101 on GigabitEthernet5/0:
   5218 packets, 513444 bytes input
   3042 packets, 369567 bytes output
```

The following sample output from the **showvlansdot1q**command displays the individual subinterface statistics and summary statistics for all the VLAN subinterfaces under the physical interface Gigabit Ethernet 5/0 that have an outer VLAN ID of 101:

```
Router# show vlans dot1q 101 GigabitEthernet 5/0 detail
GigabitEthernet5/0.101 (0)
   3220 packets, 269148 bytes input
   1008 packets, 119622 bytes output
GigabitEthernet5/0.1019999 (101/1-1000,1003-2000)
   0 packets, 0 bytes input
   3 packets, 1143 bytes output
GigabitEthernet5/0.1011001 (101/1001)
   1005 packets, 122556 bytes input
   1023 packets, 125136 bytes output
GigabitEthernet5/0.1011002 (101/1002)
   1005 packets, 122556 bytes input
   1008 packets, 123666 bytes output
Total statistics for 802.1Q VLAN 101 on GigabitEthernet5/0:
   5230 packets, 514260 bytes input
   3042 packets, 369567 bytes output
```

The following sample output from the **showvlansdot1q**command displays the statistics for an outer VLAN and inner VLAN ID combination. This is a summary that displays the total for all the subinterfaces on the router that are configured with the specified IDs.

Note When multiple inner VLANs are used, the statistics displayed are at subinterface-level granularity, not VLAN-ID granularity. For example, when a range of inner VLAN IDs is assigned to a subinterface, the statistics are reported only at the subinterface level. Statistics are not available for each inner VLAN ID.

```
Router# show vlans dot1q 101 second-dot1q 1001 detail
GigabitEthernet5/0.1011001 (101/1001)
   1005 packets, 122556 bytes input
   1023 packets, 125136 bytes output
Total statistics for Outer/Inner VLAN 101/1001:
   1005 packets, 122556 bytes input
   1023 packets, 125136 bytes output
```

The following sample output from the **showvlansdot1q**command displays the statistics for a specific outer VLAN ID of 301 and an inner VLAN ID of any. This is a summary that displays the total for all of the subinterfaces on the router that are configured with the specified IDs.

```
Router# show vlans dot1q 301 second-dot1q any
GigabitEthernet5/0.301999 (301/any)
   0 packets, 0 bytes input
   3 packets, 1128 bytes output
Total statistics for Outer/Inner VLAN 301/"any":
   0 packets, 0 bytes input
   3 packets, 1128 bytes output
```

QinQ Subsystem Information: Example

The following sample output from the **showvlansdot1q**command displays some internal information about the QinQ subsystem and is used for troubleshooting purposes (typically by Cisco engineers):

```
Router# show vlans dot1q internal
Internal VLAN representation on FastEthernet0/0:
VLAN Id: 1    (.1Q, Fa0/0)
VLAN Id: 201  (.1Q-in-.1Q tree, 3 elements)
  Inner VLAN Id: (0   -0   ) Fa0/0.201
  dot1q software subblock bitlist missing
  Inner VLAN Id: (2001-2001) Fa0/0.2012001
  2001
  Inner VLAN Id: (2002-2002) Fa0/0.2012002
  2002
  "any" Fa0/0.201999
VLAN Id: 401  (.1Q-in-.1Q tree, 3 elements)
  Inner VLAN Id: (0   -0   ) Fa0/0.401
  dot1q software subblock bitlist missing
  Inner VLAN Id: (100 -900 ) Fa0/0.4019999
  100-900,1001-2000
  Inner VLAN Id: (1001-2000) Fa0/0.4019999
  100-900,1001-2000
Internal VLAN representation on GigabitEthernet5/0:
VLAN Id: 1    (.1Q, Gi5/0)
VLAN Id: 101  (.1Q-in-.1Q tree, 5 elements)
  Inner VLAN Id: (0   -0   ) Gi5/0.101
  dot1q software subblock bitlist missing
  Inner VLAN Id: (1   -1000) Gi5/0.1019999
  1-1000,1003-2000
  Inner VLAN Id: (1001-1001) Gi5/0.1011001
  1001
  Inner VLAN Id: (1002-1002) Gi5/0.1011002
  1002
  Inner VLAN Id: (1003-2000) Gi5/0.1019999
  1-1000,1003-2000
VLAN Id: 301  (.1Q-in-.1Q tree, 1 elements)
  Inner VLAN Id: (0   -0   ) Gi5/0.301
  dot1q software subblock bitlist missing
  "any" Gi5/0.301999
```

Cisco ASR 1000 Series Router: Example

The following is an example of the output displayed on the Cisco ASR 1000 series router only. For the Cisco ASR 1000 series router only, the command output includes the total number of packets dropped from the SPA due to ingress over subscription on the VLAN.

```
Router# show vlans dot1q gigabitEthernet 0/0/3.1
GigabitEthernet0/0/3.1 (0)
   133279760 packets, 8529904640 bytes input
   0 packets, 0 bytes output
   121997683 oversub packet drops
```

The table below describes the significant fields shown in the display.

Table 7: show vlans dot1q (Cisco ASR 1000 Series Router) Field Descriptions

Field	Description
GigabitEthernet0/0/3.1	Statistics are shown for Gigabit Ethernet subinterface 0/0/3.1.
packets	Number of packets encapsulated by the 802.1Q QinQ VLAN.
bytes input	Number of bytes input.
bytes output	Number of bytes output.
oversub packet drops	Number of packets dropped from the SPA due to ingress over subscription on the VLAN.

Related Commands

Command	Description
encapsulation dot1q	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.
vlan (VLAN)	Configures a specific VLAN.
vlan database	Enters VLAN configuration mode.

show vlans tokenring

To display Token Ring VLANs, use the **showvlanstokenring** command in user EXEC or privileged EXEC mode.

show vlans tokenring

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was modified. This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to use the **showvlanstokenring** command. The fields shown in the display are self-explanatory.

Router# **showvlanstokenring**

When the **showvlanstokenring** command is executed on a device with the Token Ring configurations, the output consists of a list of Token Ring interfaces with VLAN configuration.

Related Commands

Command	Description
encapsulation dot1q	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.
show vlans	Displays VLAN subinterfaces.
show vlans dot1q	Displays statistics about 802.1Q VLAN subinterfaces.

show vlan-switch

To display VLAN information, use the **showvlan-switch** command in user EXEC or privileged EXEC mode.

show vlan-switch [{**brief** | **id** *vlan* | **internal usage** | **name** *name* | **summary**}]

Syntax Description

brief	(Optional) Displays only a single line for each VLAN, identifying the VLAN, status, and ports.
id *vlan*	(Optional) Displays information about a single VLAN identified by VLAN ID number. The range is from 1 to 1005.
internal usage	(Optional) Displays VLAN internal usage information.
name *name*	(Optional) Displays information about a single VLAN identified by VLAN name. Valid values are ASCII strings from 1 to 32 characters.
summary	(Optional) Displays VLAN summary information.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XT	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Each Ethernet switch port and Ethernet repeater group belongs to only one VLAN. Trunk ports can be on multiple VLANs.

Examples

The following is sample output from the example **showvlan-switch** command, which displays the VLAN parameters for all VLANs within the administrative domain:

```
Router# show vlan-switch
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa4/0, Fa4/1, Fa4/2, Fa4/3
                                                Fa4/4, Fa4/5, Fa4/6, Fa4/7
                                                Fa4/8, Fa4/9, Fa4/10, Fa4/11
                                                Fa4/12, Fa4/13, Fa4/14, Fa4/15
                                                Fa4/16, Fa4/17, Fa4/18, Fa4/19
                                                Fa4/20, Fa4/21, Fa4/22, Fa4/23
                                                Fa4/24, Fa4/25, Fa4/26, Fa4/27
                                                Fa4/28, Fa4/29, Fa4/30, Fa4/31
                                                Fa4/32, Fa4/33, Fa4/34, Fa4/35
                                                Gi4/0, Gi4/1, Po1
2    VLAN0002                         active
3    VLAN0003                         active
5    VLAN0005                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
```

```
1005 trnet-default                        active
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
5    enet  100005     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      0      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
```

The table below describes the significant fields shown in the display.

Table 8: show vlan Field Descriptions

Field	Description
VLAN	VLAN number.
Name	Name of the VLAN, if configured.
Status	Status of the VLAN (active or suspend).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.
BridgeNo	Bridge number for the VLAN, if applicable.
Stp	Spanning-Tree Protocol type used on the VLAN.
BrdgMode	Bridging mode for this VLAN--Possible values are source-route bridging (SRB) and source-route transparent bridging (SRT); the default is SRB.
Trans1, Trans2	Types of translational bridges that the VLAN in the VLAN column is configured to translate to. Translational bridge VLANs must be a VLAN media type different from the affected VLAN; if two VLANs are specified, each one must be a different type. Common VLAN types include Ethernet (enet), FDDI (fdnet), and Token Ring (tnet). The numbers in the Trans1 and Trans2 columns refer to the VLAN ID numbers of the translational bridge VLANs. **Note** The term *VLAN translation* is also used in Cisco configuration guides for mapping specific VLANs in a given trunk to another VLAN that is of the same media type. In this context the term *VLAN translation* refers to a form of VLAN mapping that is using the term *VLAN translation* to describe it.

Related Commands

Command	Description
vlan (**VLAN)**	Configures specific VLANs.

show vtp

To display general information about the VLAN Trunking Protocol (VTP) management domain, status, and counters, use the**showvtp** command in privileged EXEC mode.

```
show vtp{counters|interfacetype/number|status|password|devices|[{conflicts}]}
```

Syntax Description

counters	Displays the VTP counters for the switch.
interface	Displays information for all interfaces.
type / number	(Optional) A specific interface.
status	Displays general information about the VTP management domain.
password	Displays VTP password in VTP version 3 domain.
devices	Displays VTP version 3 domain information.
conflicts	(Optional) Displays only devices that have conflicting servers in a VTP version 3 domain.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2(8)SA4	This command was introduced.
12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	This command on the Supervisor Engine 2 was extended to Cisco IOS Release12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	The**password**,**devices**, and **conflicts** keywords were added to support VTP version 3 on the Cisco 7600 series routers.
12.2(33)SXI	The output for counters and status were updated to include VTPv3 information.

Usage Guidelines

In the output of the **showvtpstatus** command, the last modified time is of the modifier itself. For example, the time displayed in the line “Configuration last modified by 7.0.22.11 at 5-5-06 05:51:49”, is the time that the modifier (7.0.22.11) last modified the VLAN configuration.

Examples

The following is sample output from the **showvtpcounters** command:

```
Router# show vtp counters
VTP statistics:
Summary advertisements received : 0
Subset advertisements received : 0
Request advertisements received : 0
Summary advertisements transmitted : 6970
Subset advertisements transmitted : 0
Request advertisements transmitted : 0
Number of config revision errors : 0
Number of config digest errors : 0
Number of V1 summary errors : 0
VTP pruning statistics:
Trunk             Join Transmitted Join Received    Summary advts received from
                                          non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
Gi1/11            0                0                0
Gi8/10            0                0                0
Gi8/15            0                0                0
Gi8/16            0                0                0
Fa3/1             0                0                0
Fa3/2             0                0                0
Router#
```

This example shows how to display only those lines in the **showvtp** output that contain the word Summary:

```
Router# show vtp counters | include Summary
Summary advertisements received    : 1
Summary advertisements transmitted : 32
Trunk            Join Transmitted Join Received    Summary advts received from
Router#
```

This example shows how to display general information about the VTP management domain:

```
Router# 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 8-7-06 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
Router#
```

The table below describes the significant fields shown in the display.

Table 9: show vtp counters Field Descriptions

Field	Description
Summary advertisements received	Number of summary advertisements received by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update time stamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements received	Number of subset advertisements received by this switch on its trunk ports. Subset advertisements contain all the VTP information for one or more VLANs.
Request advertisements received	Number of advertisement requests received by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Summary advertisements transmitted	Number of summary advertisements sent by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update time stamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements transmitted	Number of subset advertisements sent by this switch on its trunk ports. Subset advertisements contain all the VTP information for one or more VLANs.
Request advertisements transmitted	Number of advertisement requests sent by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Number of config revision errors	Number of revision errors. Whenever you define a new VLAN, delete an existing VLAN, suspend or resume an existing VLAN, or modify the parameters on an existing VLAN, the configuration revision number of the switch increments. Revision errors increment whenever the switch receives an advertisement whose revision number matches the revision number of the switch, but the message digest algorithm 5 (MD5) values do not match. This error indicates that the VTP password in the two switches is different, or the switches have different configurations. These errors indicate that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.
Number of config digest errors	Number of MD5 errors. Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the switch do not match. This error usually indicates that the VTP passwords in the two switches are different. To solve this problem, make sure the VTP password on all switches is the same. These errors indicate that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.

Field	Description
Number of V1 summary errors	Number of version 1 errors. Version 1 summary errors increment whenever a switch in VTP V2 mode receives a VTP version 1 frame. These errors indicate that at least one neighboring switch is either running VTP version 1 or VTP version 2 with V2-mode disabled. To solve this problem, change the configuration of the switches in VTP V2-mode to disabled.
Trunk	Trunk port participating in VTP pruning.
Join Transmitted	Number of VTP pruning messages transmitted on the trunk.
Join Received	Number of VTP pruning messages received on the trunk.
Summary advts received from non-pruning-capable device	Number of VTP summary messages received on the trunk from devices that do not support pruning.

The following is sample output from the **showvtpstatus** command for VTP version 1 and VTP version 2:

```
Router# show vtp status
VTP Version                     : 3 (capable)
Configuration Revision          : 1
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 37
VTP Operating Mode              : Server
VTP Domain Name                 : [smartports]
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x26 0xEE 0x0D 0x84 0x73 0x0E 0x1B 0x69
Configuration last modified by 172.20.52.19 at 7-25-08 14:33:43
Local updater ID is 172.20.52.19 on interface Gi5/2 (first layer3 interface fou)
VTP version running             : 2
```

The table below describes the significant fields shown in the display.

Table 10: show vtp status Field Descriptions

Field	Description
VTP Version	Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers Displays the VTP version operating on the switch. By default, switches implement version 1. Catalyst Switches Displays the VTP version operating on the switch. By default, Catalyst 2900 and 3500 XL switches implement version 1 but can be set to version 2.
Configuration Revision	Current configuration revision number on this switch.

Field	Description
Maximum VLANs supported locally	Maximum number of VLANs supported locally.
Number of existing VLANs	Number of existing VLANs.
VTP Operating Mode	Displays the VTP operating mode, which can be server, client, or transparent. • Server--A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch guarantees that it can recover all VLAN information in the current VTP database from nonvolatile storage after reboot. By default, every switch is a VTP server. • Client--A switch in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not transmit VTP advertisements until it receives advertisements to initialize its VLAN database. • Transparent--A switch in VTP transparent mode is disabled for VTP, does not transmit advertisements or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received. The configuration of multi-VLAN ports causes the switch to automatically enter transparent mode. • Off--When VTP is disabled using off mode, the switch behaves the same as in VTP transparent mode except that VTP advertisements are not forwarded. **Note** Catalyst 2912MF, 2924M, and 3500 XL switches support up to 250 VLANs. All other Catalyst 2900 XL switches support up to 64 VLANs. For Catalyst 2912MF, 2924M, and 3500 XL switches, if you define more than 250 VLANs or if the switch receives an advertisement that contains more than 250 VLANs, the switch automatically enters VTP transparent mode and operates with the VLAN configuration preceding the one that sent it into transparent mode. For all other Catalyst 2900 XL switches, if you define more than 64 VLANs or if the switch receives an advertisement that contains more than 64 VLANs, the switch automatically enters VTP transparent mode and operates with the VLAN configuration preceding the one that sent it into transparent mode.
VTP Domain Name	Name that identifies the administrative domain for the switch.
VTP Pruning Mode	Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers VTP pruning mode is not supported on the Cisco 2600, Cisco 3600, and 3700 series routers. Catalyst Switches, Cisco 7600 Series Routers Displays whether pruning is enabled or disabled. Enabling pruning on a VTP server enables pruning for the entire management domain. Pruning restricts flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.

Field	Description
VTP V2 Mode	Displays if VTP version 2 mode is enabled. All VTP version 2 switches operate in version 1 mode by default. Each VTP switch automatically detects the capabilities of all other VTP devices. A network of VTP devices should be configured to version 2 only if all VTP switches in the network can operate in version 2 mode.
VTP Traps Generation	Displays whether VTP traps are transmitted to a network management station.
MD5 digest	16-byte checksum of the VTP configuration.
Configuration last modified	Displays the date and time of the last configuration modification. Displays the IP address of the switch that caused the configuration change to the database.

The following is sample output from the **showvtpstatus** command for all three VTP versions on the Cisco 7600 series routers running Release 12.2(33)SRC and later.

This example shows how to verify the configuration when the device is running VTP version 1:

```
Router# show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : Lab_Network
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : 0016.9c6d.5300
Configuration last modified by 127.0.0.12 at 10-18-07 10:12:42
Local updater ID is 127.00.12 at 10-18-07 10:2:42
Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum number of existing VLANs : 5
Configuration Revision          : 1
MD5 digest                      : 0x92 0xF1 0xE8 0x52 0x2E ox5C 0x36 0x10 0x70 0x61 0xB8
                              0x24 0xB6 0x93 0x21 0x09
Router#
```

This example shows how to verify the configuration when the device is running VTP version 2:

```
Router# show vtp status
VTP Version capable          : 1 to 3
VTP version running          : 2
VTP Domain Name              : Lab_Network
VTP Pruning Mode             : Disabled
VTP Traps Generation         : Disabled
Device ID                    : 0012.44dc.b800
Configuration lst modified by 127.0.0.12 at 10-18-07 10:38:45
Local updater ID is 127.0.0.12 on interface EO 0/0 (first interface found)
Feature VLAN:
--------------
VTP Operating Mode           : Server
Maximum VLANs supported locally: 1005
Number of existing VLANs     : 1005
Configuration Revision       : 1
MD5 digest                   : 0x2E 0x6B 0x99 0x58 0xA2 0x4F 0xD5 0x150x70 0x61 0xB8
                       0x24 0xB6 0x93 0x21 0x09
Router#
```

This example shows how to verify the configuration when the device is running VTP version 3:

```
Router# show vtp status
VTP Version capable          : 1 to 3
VTP version running          : 3
VTP Domain Name              : Lab_Network
VTP Pruning Mode             : Disabled
VTP Traps Generation         : Disabled
Device ID                    : 0012.44dc.b800
Feature VLAN:
--------------
VTP Operating Mode              : Server
Number of existing VLANs        : 1005
Number of existing extended VLANs: 3074
Configuration Revision          : 18
Primary ID                      : 0012.4371.9ec0
Primary Description             :
Router#
```

The table below describes the significant fields shown in the displays.

Table 11: show vtp status Field Descriptions (Cisco 7600 Series Routers Release 12.2(33)SRC and Later)

Field	Description
VTP Version capable	Versions of VTP that the device is capable of running.
VTP Version running	Version of VTP that the device is running.
VTP Domain Name	Name that identifies the administrative domain for the device.
VTP Pruning Mode	Displays whether pruning is enabled or disabled. Enabling pruning on a VTP server enables pruning for the entire management domain. Pruning restricts flooded traffic to those trunk lines that the traffic must use to access the appropriate network devices.
VTP Traps Generation	Displays whether VTP traps are transmitted to a network management station.
Device ID	MAC address of the local device.
Configuration last modified Configuration lst modified	Displays the date and time of the last configuration modification. Displays the IP address of the switch that caused the configuration change to the database.
VTP Operating Mode	VTP Mode (Client, Server, Transparent, Off) listed by feature type.
Maximum VLANs supported locally	Maximum number of VLANs supported locally.
Maximum number of existing VLANs	Number of existing VLANs.
Number of existing extended VLANs	Number of existing extended VLANs.
Configuration Revision	Configuration revision number for the specific feature.
Primary ID	MAC address of primary server.
Primary Description	Name of primary server.

Field	Description
MD5 digest	32-bit checksum of the VTP configuration.

This example shows how to display information for a specific interface:

```
Router# show vtp interface GigabitEthernet2/4
Interface              VTP Status
------------------------------------
GigabitEthernet2/4     enabled
```

This example shows how a password is displayed when it is configured using the **hidden** keyword (VTP version 3 only):

```
Router# show vtp password
VTP Password: 89914640C8D90868B6A0D8103847A733
Router#
```

This example shows how to display information about all VTP devices in the domain:

```
Router# show vtp devices
Gathering information from the domain, please wait.
VTP Database Conf switch ID      Primary Server Revision  System Name
             lict
------------ ---- -------------- ------------------------ ------------------
VLAN         Yes  00b0.8e50.d000 000c.0412.6300 12354     main.cisco.com
MST          No   00b0.8e50.d000 0004.AB45.6000 24        main.cisco.com
VLAN         Yes  000c.0412.6300=000c.0412.6300 67        querty.cisco.com
```

The table below describes the significant fields shown in the display.

Table 12: show vtp devices Field Descriptions

Field	Description
VTP Database	Displays the feature (database) type (VLAN or MST) of each server.
Conflict	Yes is displayed in this column if the server is in conflict with the local server for the feature. A conflict is detected when two devices in the same domain do not have the same primary server for the given database.
Switch ID	The MAC address of the server.
Primary Server	The MAC address of the primary server for the device identified in the Switch ID column. If a device is configured with a database that it originated, and equal sign (=) appears between the Primary Server field and the Switch ID field.
Revision	Revision number of the VTP database.
System Name	String provided to more easily identify the system.

Related Commands

Command	Description
clear vtp counters	Clears the VTP and pruning counters.

Command	Description
vtp	Configures the VTP mode.

shutdown vlan

To shut down local traffic on a specified VLAN, use the **shutdownvlan** command in global configuration mode. To restart local traffic on the VLAN, use the **no** form of this command.

shutdown vlan *vlan-id*
no shutdown vlan *vlan-id*

Syntax Description

vlan-id	VLAN number of the VLAN to be locally shut down; valid values are from 2 to 1001.

Command Default

Local traffic on a specified VLAN is not shut down.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command does not support extended-range VLANs.

Examples

This example shows how to shut down traffic on VLAN 2:

```
Router(config)#
shutdown vlan 2
```

snmp trap mac-notification change

To enable the Simple Network Management Protocol (SNMP) trap notification on a LAN port when MAC addresses are added to or removed from the address table , use the **snmptrapmac-notificationchange** command in interface configuration mode. To disable the SNMP trap notification on a LAN port when MAC addresses are added to or removed from the address table , use the **no** form of this command.

snmp trap mac-notification change [{**added** | **removed**}]
no snmp trap mac-notification change

Syntax Description

added	(Optional) Sends notification only when a MAC address is added to the table.
removed	(Optional) Sends notification only when a MAC address is removed to the table.

Command Default

The SNMP trap notification is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Examples

The following example shows how to enable the SNMP trap notification on a LAN port when MAC addresses are added to the address table :

```
Router(config-if)# snmp trap mac-notification change
 added
```

The following example shows how to enable the SNMP trap notification on a LAN port when MAC addresses are removed from the address table :

```
Router(config-if)# snmp trap mac-notification change
 removed
```

The following example shows how to disable the SNMP trap notification on a LAN port:

```
Router(config-if)# no snmp trap mac-notification change
```

Related Commands

Command	Description
mac-address-table notification change	Sends a notification of the dynamic changes to the MAC address table.

source interface

To configure more than one WAN interface in a single Encapsulated Remote Switched Port Analyzer (ERSPAN) session, use the **source interface** command in ERSPAN monitor source session configuration mode.

To disable the WAN interface, use the **no** form of the command.

source interface {**Gigabit Ethernet** *interface-number* */port* */interface-number* **:***interface-number* | **Multilink** *multilink-number* */port* */interface-number* **:** *interface-number* | **POS** *pos-number* */port* */interface-number* **:** *interface-number* | **Port-channel** *interface-number* */port* */interface-number* **:** *interface-number* | [{**,** | **-**}] | **Serial** *interface-number* *port* */interface-number* **:** *interface-number* | **Tunnel** *interface-number* */port* */interface-number* **:** *interface-number*} [{**both** | **rx** | **tx**}]
no source interface {**Gigabit Ethernet** *interface-number* */port* */interface-number* **:***interface-number* | **Multilink** *multilink-number* */port* */interface-number* **:** *interface-number* | **POS** *pos-number* */port* */interface-number* **:** *interface-number* | **Port-channel** *interface-number* */port* */interface-number* **:** *interface-number* | [{**,** | **-**}] | **Serial** *interface-number* *port* */interface-number* **:** *interface-number* | **Tunnel** *interface-number* */port* */interface-number* **:** *interface-number*} [{**both** | **rx** | **tx**}]

Syntax Description

gigabitethernet *interface*	GigabitEthernet IEEE 802.3z interface.
multilink *multilink-number*	Multilink-group interface.
pos *pos-number*	Packet over SONET. POS interface number
,	Specifies another interface.
-	Specifies a range of interfaces.
both	Monitors the traffic received and transmitted on an interface.
rx	Monitors traffic received on an interface.
tx	Monitors traffic transmitted on an interface.
port-channel	Specifies the Ethernet Channel interface.
/ *interface-number*	Starting interface number.
/port	Port number.
:*interface-number*	Ending interface number.
serial	Specifies the Serial interface.
tunnel	Specifies the Tunnel interface.

Command Modes

ERSPAN monitor source session configuration mode (config-mon-erspan-src)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was modified. The **Multilink**, **POS**, and **Serial** keywords were added.

Usage Guidelines

- When you configure multiple interfaces in a session, list each interface along with its port and interface number, and separate each interface using a comma.
- You can configure more than one WAN interface in a single ERSPAN source monitor session by separating different WAN interfaces using a comma. You can configure 20 WAN interfaces separated by a comma and an unlimited interfaces using hyphens.
- The **Serial** keyword is displayed only if a serial interface is configured on the router.
- If the **Source interface Serial** command is configured, you cannot configure the **source vlan** command under the same ERSPAN source monitor session.
- You cannot configure a virtual LAN (VLAN) in an ERSPAN monitoring session on a WAN interface.

Examples

The following example shows how to configure more than one WAN interface in a single ERSPAN source monitor session. Multiple interfaces have been separated by commas.

```
Router# configure terminal
Router(config)# monitor session 100 type erspan-source
Router(config-mon-erspan-src)# source interface serial 0/1/0:0, serial 0/1/0:6
```

Related Commands

Command	Description
source vlan	Associates the ERSPAN source session number with the source ports.

spanning-tree portfast bpdufilter default

To enable bridge protocol data unit (BPDU) filtering by default on all PortFast ports, use the **spanning-treeportfastbpdufilterdefault**command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree portfast bpdufilter default
no spanning-tree portfast bpdufilter default

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **spanning-treeportfastbpdufilter** command enables BPDU filtering globally on PortFast ports. BPDU filtering prevents a port from sending or receiving any BPDUs.

You can override the effects of the **portfastbpdufilterdefault** command by configuring BPDU filtering at the interface level.

Note Be careful when enabling BPDU filtering. The feature's functionality is different when you enable it on a per-port basis or globally. When enabled globally, BPDU filtering is applied only on ports that are in an operational PortFast state. Ports send a few BPDUs at linkup before they effectively filter outbound BPDUs. If a BPDU is received on an edge port, it immediately loses its operational PortFast status and BPDU filtering is disabled. When enabled locally on a port, BPDU filtering prevents the Cisco 7600 series router from receiving or sending BPDUs on this port.

Caution Be careful when using this command. Using this command incorrectly can cause bridging loops.

Examples

This example shows how to enable BPDU filtering by default:

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

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree bpdufilter	Enables BPDU filtering on the interface.

spanning-tree backbonefast

To enable BackboneFast to allow a blocked port on a switch to change immediately to a listening mode, use the **spanning-treebackbonefast** command in global configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree backbonefast
no spanning-tree backbonefast

Syntax Description

This command has no arguments or keywords.

Command Default

BackboneFast is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(15)ZJ	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

BackboneFast should be enabled on all of the Cisco routers containing an Ethernet switch network module. BackboneFast provides for fast convergence in the network backbone after a spanning-tree topology change. It enables the switch to detect an indirect link failure and to start the spanning-tree reconfiguration sooner than it would under normal spanning-tree rules.

Use the **showspanning-tree** privileged EXEC command to verify your settings.

Examples

The following example shows how to enable BackboneFast on the switch:

```
Router(config)# spanning-tree backbonefast
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

spanning-tree bpdufilter

To enable bridge protocol data unit (BPDU) filtering on the interface, use the **spanning-treebpdufilter**command in interface configuration or template configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree bpdufilter {**enable** | **disable**}
no spanning-tree bpdufilter

Syntax Description

enable	Enables BPDU filtering on this interface.
disable	Disables BPDU filtering on this interface.

Command Default

The setting that is already configured when you enter the **spanning-treeportfastbpdufilterdefault** command .

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.2(2)E	This command was integrated into Cisco IOS Release 15.2(2)E. This command is supported in template configuration mode.
Cisco IOS XE Release 3.6E	This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.

Usage Guidelines

⚠ **Caution** Be careful when you enter the **spanning-treebpdufilterenable** command. Enabling BPDU filtering on an interface is similar to disabling the spanning tree for this interface. If you do not use this command correctly, you might create bridging loops.

Entering the **spanning-treebpdufilterenable** command to enable BPDU filtering overrides the PortFast configuration.

When configuring Layer 2-protocol tunneling on all the service-provider edge switches, you must enable spanning-tree BPDU filtering on the 802.1Q tunnel ports by entering the **spanning-treebpdufilterenable** command.

BPDU filtering prevents a port from sending and receiving BPDUs. The configuration is applicable to the whole interface, whether it is trunking or not. This command has three states:

- **spanning-tree bpdufilter enable** -- Unconditionally enables BPDU filtering on the interface.
- **spanning-tree bpdufilter disable** -- Unconditionally disables BPDU filtering on the interface.
- **no spanning-tree bpdufilter** -- Enables BPDU filtering on the interface if the interface is in operational PortFast state and if you configure the **spanning-treeportfastbpdufilterdefault** command.

Use the **spanning-treeportfastbpdufilterdefault**command to enable BPDU filtering on all ports that are already configured for PortFast.

Examples

This example shows how to enable BPDU filtering on this interface:

```
Router(config-if)# spanning-tree bpdufilter enable
Router(config-if)#
```

The following example shows how to enable BPDU filtering on an interface using interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# spanning-tree bpdufilter enable
Device(config-template)# end
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree portfast bpdufilter default	Enables BPDU filtering by default on all PortFast ports.

spanning-tree bpduguard

To enable bridge protocol data unit (BPDU) guard on the interface, use the **spanning-tree bpduguard** command in interface configuration and template configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree bpduguard {**enable** | **disable**}
no spanning-tree bpduguard

Syntax Description

enable	Enables BPDU guard on this interface.
disable	Disables BPDU guard on this interface.

Command Default

The setting that is already configured when you enter the **spanning-treeportfast bpduguard default** command .

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	**Modification**
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.2(2)E	This command was integrated into Cisco IOS Release 15.2(2)E. This command is supported in template configuration mode.
Cisco IOS XE Release 3.6E	This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.

Usage Guidelines

BPDU guard prevents a port from receiving BPDUs. Typically, this feature is used in a service-provider environment where the network administrator wants to prevent an access port from participating in the spanning tree. If the port still receives a BPDU, it is put in the error-disabled state as a protective measure. This command has three states:

- **spanning-tree bpduguard enable** -- Unconditionally enables BPDU guard on the interface.
- **spanning-tree bpduguard disable** -- Unconditionally disables BPDU guard on the interface.
- **no spanning-tree bpduguard** --E nables BPDU guard on the interface if it is in the operational PortFast state and if the **spanning-treeportfastbpduguarddefault** command is configured.

Examples

This example shows how to enable BPDU guard on this interface:

```
Router(config-if)# spanning-tree bpduguard enable
Router(config-if)#
```

The following example shows how to enable BPDU guard on an interface using interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# spanning-tree bpduguard enable
Device(config-template)# end
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree portfast bpduguard default	Enables BPDU guard by default on all PortFast ports.

spanning-tree bridge assurance

To enable Bridge Assurance on all network ports on the switch, use the **spanning-treebridgeassurance**command in global configuration mode. To disable Bridge Assurance, use the **no** form of this command.

spanning-tree bridge assurance
no spanning-tree bridge assurance

Syntax Description

This command has no arguments or keywords.

Command Default

Bridge Assurance is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXI	Support for this command was introduced.

Usage Guidelines

Bridge Assurance protects against a unidirectional link failure or other software failure and a device that continues to forward data traffic when it is no longer running the spanning tree algorithm.

Bridge Assurance is enabled only on spanning tree network ports that are point-to-point links. Both ends of the link must have Bridge Assurance enabled. If the device on one side of the link has Bridge Assurance enabled and the device on the other side either does not support Bridge Assurance or does not have this feature enabled, the connecting port is blocked.

Disabling Bridge Assurance causes all configured network ports to behave as normal spanning tree ports.

Examples

This example shows how to enable Bridge Assurance on all network ports on the switch:

```
Router(config)#
spanning-tree bridge assurance
Router(config)#
```

This example shows how to disable Bridge Assurance on all network ports on the switch:

```
Router(config)#
no spanning-tree bridge assurance
Router(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

spanning-tree cost

To set the path cost of the interface for Spanning Tree Protocol (STP) calculations, use the **spanning-treecost** command in interface configuration or template configuration mode. To revert to the default value, use the **no** form of this command.

spanning-tree cost *cost*
no spanning-tree cost

Syntax Description

cost	Path cost; valid values are from 1 to 200000000 for Cisco IOS Releases 12.1(3a)E and later releases and from 1 to 65535 for Cisco IOS releases prior to Cisco IOS Release 12.1(3a)E.

Command Default

The default path cost is computed from the bandwidth setting of the interface; default path costs are:

Ethernet: 100 16-Mb Token Ring: 62 FDDI: 10 FastEthernet: 10 ATM 155: 6 GigibitEthernet: 1 HSSI: 647

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 family switches.
12.1(3a)E	This command was modified to support 32-bit path cost.
12.2(2)XT	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.2(2)E	This command was integrated into Cisco IOS Release 15.2(2)E. This command is supported in template configuration mode.
Cisco IOS XE Release 3.6E	This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.

Usage Guidelines

When you specify a value for the cost argument, higher values indicate higher costs. This range applies regardless of the protocol type specified.

Examples

The following example shows how to access an interface and set a path cost value of 250 for the spanning tree VLAN associated with that interface:

```
Router(config)# interface ethernet 2/0
Router(config-if)# spanning-tree cost 250
```

The following example shows how to set a path cost value of 250 for the spanning tree VLAN associated with an interface using an interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# spanning-tree cost 250
Device(config-template)# end
```

Related Commands

Command	Description
show spanning -tree	Displays spanning-tree information for the specified spanning-tree instances.
spanning -treeport-priority	Sets an interface priority when two bridges tie for position as the root bridge.
spanning-tree portfast (global)	Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire.
spanning-tree portfast (interface)	Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire.
spanning -treeuplinkfast	Enables the UplinkFast feature.
spanning -treevlan	Configures STP on a per-VLAN basis.

spanning-tree etherchannel guard misconfig

To display an error message when a loop due to a channel misconfiguration is detected, use the **spanning-treeetherchannelguardmisconfig** command in global configuration mode. To disable the error message, use the **no** form of this command.

spanning-tree etherchannel guard misconfig
no spanning-tree etherchannel guard misconfig

Syntax Description

This command has no arguments or keywords.

Command Default

Error messages are displayed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

EtherChannel uses either Port Aggregation Protocol (PAgP) or Link Aggregation Control Protocol (LACP) and does not work if the EtherChannel mode of the interface is enabled using the **channel-group** group-number mode on command.

The **spanning-treeetherchannelguardmisconfig** command detects two types of errors: misconfiguration and misconnection errors. A misconfiguration error is an error between the port-channel and an individual port. A misconnection error is an error between a switch that is channeling more ports and a switch that is not using enough Spanning Tree Protocol (STP) Bridge Protocol Data Units (BPDUs) to detect the error. In this case, the switch will only error disable an EtherChannel if the switch is a nonroot switch.

When an EtherChannel-guard misconfiguration is detected, this error message displays:

```
msgdef(CHNL_MISCFG, SPANTREE, LOG_CRIT, 0, "Detected loop due to etherchannel misconfiguration
 of %s %s")
```

To determine which local ports are involved in the misconfiguration, enter the **showinterfacesstatuserr-disabled** command. To check the EtherChannel configuration on the remote device, enter the **showetherchannelsummary**command on the remote device.

After you correct the configuration, enter the **shutdown** and the **noshutdown** commands on the associated port-channel interface.

Examples

This example shows how to enable the EtherChannel-guard misconfiguration:

Router(config)# **spanning-treeetherchannelguardmisconfig**

Router(config)#

Related Commands

Command	Description
show etherchannel summary	Displays the EtherChannel information for a channel.
show interfaces status err-disabled	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.
shutdown	Disables an interface.

spanning-tree extend system-id

To enable the extended-system ID feature on chassis that support 1024 MAC addresses, use the **spanning-treeextendsystem-id** command in global configuration mode. To disable the extended system identification, use the **no** form of this command.

spanning-tree extend system-id
no spanning-tree extend system-id

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled on systems that do not provide 1024 MAC addresses.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The Cisco 7600 series router can support 64 or up to 1024 MAC addresses. For a Cisco 7600 series router with 64 MAC addresses, STP uses the extended-system ID and a MAC address to make the bridge ID unique for each VLAN.

You cannot disable the extended-system ID on a Cisco 7600 series router that supports 64 MAC addresses.

Enabling or disabling the extended-system ID updates the bridge IDs of all active Spanning Tree Protocol (STP) instances, which might change the spanning-tree topology.

Examples

This example shows how to enable the extended-system ID:

```
Router(config)# spanning-tree extend system-id
Router(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

spanning-tree guard

To enable or disable the guard mode, use the **spanning-treeguard**command in interface configuration and template configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree guard {**loop** | **root** | **none**}
no spanning-tree guard

Syntax Description

loop	Enables the loop-guard mode on the interface.
root	Enables root-guard mode on the interface.
none	Sets the guard mode to none.

Command Default

Guard mode is disabled.

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.2(2)E	This command was integrated into Cisco IOS Release 15.2(2)E. This command is supported in template configuration mode.
Cisco IOS XE Release 3.6E	This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.

Examples

This example shows how to enable root guard:

```
Device(config-if)# spanning-tree guard root
Device(config-if)#
```

The following example shows how to enable root guard on an interface using an interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# spanning-tree guard root
Device(config-template)# end
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree loopguard default	Enables loop guard as a default on all ports of a given bridge.

spanning-tree link-type

To configure a link type for a port, use the **spanning-treelink-type** command in the interface configuration and template configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree link-type {**point-to-point** | **shared**}
no spanning-tree link-type

Syntax Description

point-to-point	Specifies that the interface is a point-to-point link.
shared	Specifies that the interface is a shared medium.

Command Default

Link type is automatically derived from the duplex setting unless you explicitly configure the link type.

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.2(2)E	This command was integrated into Cisco IOS Release 15.2(2)E. This command is supported in template configuration mode.
Cisco IOS XE Release 3.6E	This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.

Usage Guidelines

Rapid Spanning Tree Protocol Plus (RSTP+) fast transition works only on point-to-point links between two bridges.

By default, the switch derives the link type of a port from the duplex mode. A full-duplex port is considered as a point-to-point link while a half-duplex configuration is assumed to be on a shared link.

If you designate a port as a shared link, RSTP+ fast transition is forbidden, regardless of the duplex setting.

Examples

This example shows how to configure the port as a shared link:

```
Device(config-if)# spanning-tree link-type shared
Device(config-if)#
```

The following example shows how to configure the port as a shared link using an interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# spanning-tree link-type shared
Device(config-template)# end
```

Related Commands

Command	Description
show spanning-tree interface	Displays information about the spanning-tree state.

spanning-tree loopguard default

To enable loop guard as a default on all ports of a given bridge, use the **spanning-treeloopguarddefault** command in global configuration mode. To disable loop guard, use the **no** form of this command.

spanning-tree loopguard default
no spanning-tree loopguard default

Syntax Description

This command has no arguments or keywords.

Command Default

Loop guard is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Loop guard provides additional security in the bridge network. Loop guard prevents alternate or root ports from becoming the designated port due to a failure that could lead to a unidirectional link.

Loop guard operates only on ports that are considered point to point by the spanning tree.

The individual loop-guard port configuration overrides this command.

Examples

This example shows how to enable loop guard:

```
Router(config)#
spanning-tree loopguard default
Router(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree guard	Enables or disables the guard mode.

spanning-tree mode

To switch between Per-VLAN Spanning Tree+ (PVST+), Rapid-PVST+, and Multiple Spanning Tree (MST) modes, use the **spanning-treemode** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mode [{**pvst** | **mst** | **rapid-pvst**}]
no spanning-tree mode

Syntax Description

pvst	(Optional) PVST+ mode.
mst	(Optional) MST mode.
rapid-pvst	(Optional) Rapid-PVST+ mode.

Command Default

pvst

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release XE 3.7S	This command was integrated into Cisco IOS XE Release XE 3.7S.

Usage Guidelines

Caution Be careful when using the **spanning-treemode** command to switch between PVST+, Rapid-PVST+, and MST modes. When you enter the command, all spanning-tree instances are stopped for the previous mode and are restarted in the new mode. Using this command may cause disruption of user traffic.

Examples

This example shows how to switch to MST mode:

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

This example shows how to return to the default mode (PVST+):

```
Device(config)# no spanning-tree mode
Device(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst

To set the path cost and port-priority parameters for any Multiple Spanning Tree (MST) instance (including the Common and Internal Spanning Tree [CIST] with instance ID 0), use the **spanning-treemst** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst *instance-id* {{**cost** *cost* | **port-priority** *priority*} | **pre-standard**}
no spanning-tree mst *instance-id* {{**cost** | **port-priority**} | **pre-standard**}

Syntax Description

instance-id	Instance ID number; valid values are from 0 to 15.
cost *cost*	Path cost for an instance; valid values are from 1 to 200000000.
port-priority *priority*	Port priority for an instance; valid values are from 0 to 240 in increments of 16.
pre-standard	Configures prestandard MST BPDU transmission on the interface.

Command Default

The defaults are as follows:

- *cost* depends on the port speed; the faster interface speeds indicate smaller costs. MST always uses long path costs.
- *priority* is **128**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Higher cost *cost*values indicate higher costs. When entering the *cost*, do not include a comma in the entry; for example, enter **1000**, not **1,000**.

Higher port-priority *priority*values indicate smaller priorities.

Examples

This example shows how to set the interface path cost:

```
Router(config-if)#
spanning-tree mst 0 cost 17031970
Router(config-if)#
```

This example shows how to set the interface priority:

```
Router(config-if)#
spanning-tree mst 0 port-priority 64
Router(config-if)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree port-priority	Sets an interface priority when two bridges vie for position as the root bridge.

spanning-tree mst configuration

To enter MST-configuration submode, use the **spanning-treemstconfiguration** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst configuration
no spanning-tree mst configuration

Syntax Description

This command has no arguments or keywords.

Command Default

The default value for the Multiple Spanning Tree (MST) configuration is the default value for all its parameters:

- No VLANs are mapped to any MST instance (all VLANs are mapped to the Common and Internal Spanning Tree [CIST] instance).
- The region name is an empty string.
- The revision number is 0.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release XE 3.7S	This command was integrated into Cisco IOS XE Release XE 3.7S.

Usage Guidelines

The MST configuration consists of three main parameters:

- Instance VLAN mapping--See the **instance** command
- Region name--See the **name(MSTconfigurationsubmode)** command
- Configuration revision number--See the **revision** command

The **abort** and **exit** commands allow you to exit MST configuration submode. The difference between the two commands depends on whether you want to save your changes or not.

The **exit** command commits all the changes before leaving MST configuration submode. If you do not map secondary VLANs to the same instance as the associated primary VLAN, when you exit MST-configuration submode, a warning message displays and lists the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The warning message is as follows:

```
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

The **abort** command leaves MST-configuration submode without committing any changes.

Changing an MST-configuration submode parameter can cause connectivity loss. To reduce service disruptions, when you enter MST-configuration submode, make changes to a copy of the current MST configuration. When you are done editing the configuration, you can apply all the changes at once by using the exit keyword, or you can exit the submode without committing any change to the configuration by using the abort keyword.

In the unlikely event that two users commit a new configuration at exactly at the same time, this warning message displays:

```
% MST CFG:Configuration change lost because of concurrent access
```

Examples

This example shows how to enter MST-configuration submode:

```
Device(config)# spanning-tree mst configuration
Device(config-mst)#
```

This example shows how to reset the MST configuration to the default settings:

```
Device(config)# no spanning-tree mst configuration
Device(config)#
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
name (MST)	Sets the name of an MST region.
revision	Sets the revision number for the MST configuration.
show	Verifies the MST configuration.
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst forward-time

To set the forward-delay timer for all the instances on the Cisco 7600 series router, use the **spanning-treemstforward-time**command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst forward-time *seconds*
no spanning-tree mst forward-time

Syntax Description

seconds	Number of seconds to set the forward-delay timer for all the instances on the Cisco 7600 series router; valid values are from 4 to 30 seconds.

Command Default

seconds is **15**

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to set the forward-delay timer:

```
Router(config)# spanning-tree mst forward-time 20
```

Router(config)#

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst hello-time

To set the hello-time delay timer for all the instances on the Cisco 7600 series router, use the **spanning-treemsthello-time** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst hello-time *seconds*
no spanning-tree mst hello-time

Syntax Description

seconds	Number of seconds to set the hello-time delay timer for all the instances on the Cisco 7600 series router; valid values are from 1 to 10 second s.

Command Default

2 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you do not specify the *hello-time* value, the value is calculated from the network diameter.

Examples

This example shows how to set the hello-time delay timer:

```
Router(config)# spanning-tree mst hello-time 3
```

Router(config)#

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst max-age

To set the max-age timer for all the instances on the Cisco 7600 series router, use the **spanning-treemstmax-age** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst max-age *seconds*
no spanning-tree mst max-age

Syntax Description

seconds	Number of seconds to set the max-age timer for all the instances on the Cisco 7600 series router; valid values are from 6 to 40 seconds.

Command Default

20 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to set the max-age timer:

```
Router(config)# spanning-tree mst max-age 40
```

Router(config)#

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst max-hops

To specify the number of possible hops in the region before a bridge protocol data unit (BPDU) is discarded, use the **spanning-treemstmax-hops** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst max-hops *hopnumber*
no spanning-tree mst max-hops

Syntax Description

hopnumber	Number of possible hops in the region before a BPDU is discarded; valid values are from 1 to 255 hops.

Command Default

20 hops

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXF	This command was changed to increase the maximum number of possible hops from 40 to 255 hops.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to set the number of possible hops:

```
Router(config)# spanning-tree mst max-hops 25
```

Router(config)#

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst pre-standard

To configure a port to transmit only prestandard bridge protocol data units (BPDUs), use the **spanning-treemstpre-standard** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst pre-standard
no spanning-tree mst pre-standard

Syntax Description

This command has no arguments or keywords.

Command Default

The default is to automatically detect prestandard neighbors.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Even with the default configuration, the port can receive both prestandard and standard BPDUs.

Prestandard BPDUs are based on the Cisco IOS Multiple Spanning Tree (MST) implementation that was created before the IEEE standard was finalized. Standard BPDUs are based on the finalized IEEE standard.

If you configure a port to transmit prestandard BPDUs only, the prestandard flag displays in the **showspanning-tree**commands. The variations of the prestandard flag are as follows:

- Pre-STD (or pre-standard in long format)--This flag displays if the port is configured to transmit prestandard BPDUs and if a prestandard neighbor bridge has been detected on this interface.
- Pre-STD-Cf (or pre-standard (config) in long format)--This flag displays if the port is configured to transmit prestandard BPDUs but a prestandard BPDU has not been received on the port, the autodetection mechanism has failed, or a misconfiguration, if there is no prestandard neighbor, has occurred.
- Pre-STD-Rx (or pre-standard (rcvd) in long format)--This flag displays when a prestandard BPDU has been received on the port but it has not been configured to send prestandard BPDUs. The port will send prestandard BPDUs, but we recommend that you change the port configuration so that the interaction with the prestandard neighbor does not rely only on the autodetection mechanism.

If the MST configuration is not compatible with the prestandard (if it includes an instance ID greater than 15), only standard MST BPDUs are transmitted, regardless of the STP configuration on the port.

Examples

This example shows how to configure a port to transmit only prestandard BPDUs:

```
Router(config-if)# spanning-tree mst pre-standard
Router(config-if)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst priority

To set the bridge priority for an instance, use the **spanning-treemstpriority**command in global configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree mst *instance* **priority** *priority*
no spanning-tree mst priority

Syntax Description

instance	Instance identification number; valid values are from 0 to 4094.
priority *priority*	Specifies the bridge priority; see the "Usage Guidelines" section for valid values and additional information.

Command Default

priority is **32768**

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.

Usage Guidelines

You can set the bridge priority in increments of 4096 only. When you set the priority, valid values are **0**, **4096**, **8192**, **12288**, **16384**, **20480**, **24576**, **28672**, **32768**, **36864**, **40960**, **45056**, **49152**, **53248**, **57344**, and **61440**.

You can set the *priority* to **0** to make the switch root.

You can enter *instance*as a single instance or a range of instances, for example, 0-3,5,7-9.

Examples

This example shows how to set the bridge priority:

```
Router(config)# spanning-tree mst 0 priority 4096
Router(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst root

To designate the primary and secondary root switch and set the timer value for an instance, use the **spanning-treemstroot**command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst *instance* **root** {**primary** | **secondary**} [**diameter** *diameter* [**hello-time** *seconds*]]
no spanning-tree mst *instance* **root**

Syntax Description

instance	Instance identification number; valid values are from 0 to 4094.
primary	Specifies the high enough priority (low value) to make the root of the spanning-tree instance.
secondary	Specifies the switch as a secondary root, should the primary root fail.
diameter *diameter*	(Optional) Specifies the timer values for the root switch that are based on the network diameter; valid values are fro m 1 to 7.
hello-time *seconds*	(Optional) Specifies the duration between the generation of configuration messages by the root switch.

Command Default

The spanning-tree mst root command has no default settings.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.

Usage Guidelines

You can enter *instance*as a single instance or a range of instances, for example, 0-3,5,7-9.

The **spanning-treemstrootsecondary** value is 16384.

The **diameter***diameter* and **hello-time***seconds*keywords and arguments are available for instance 0 only.

If you do not specify the *seconds*argument, the value for it is calculated from the network diameter.

Examples

This example shows how to designate the primary root switch and timer values for an instance:

```
Router(config)# spanning-tree mst 0 root primary diameter 7 hello-time 2
Router(config)# spanning-tree mst 5 root primary
Router(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.

spanning-tree mst simulate pvst (interface)

To override the global Per-VLAN Spanning Tree (PVST) simulation setting for a port, use the **spanning-treemstsimulatepvst** interface command in interface configuration mode. To return to the default PVST simulation setting, use the **no** form of this command.

spanning-tree mst simulate pvst [**disable**]
no spanning-tree mst simulate pvst

Syntax Description

disable	Disables PVST simulation on the interface.

Command Default

PVST simulation is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	Support for this command was introduced.

Usage Guidelines

PVST simulation is enabled by default so that an interface can interoperate between Multiple Spanning Tree (MST) and Rapid Per-VLAN Spanning Tree Plus (PVST+). To prevent an accidental connection to a device that does not run MST as the default Spanning Tree Protocol (STP) mode, you can disable PVST simulation. If you disable PVST simulation, the MST-enabled port moves to the blocking state once it detects it is connected to a Rapid PVST+-enabled port. This port remains in the inconsistent state until the port stops receiving Bridge Protocol Data Units (BPDUs), and then the port resumes the normal STP transition process.

Examples

This example shows how to prevent a port from automatically interoperating with a connecting device that is running Rapid PVST+:

```
Router(config)#
interface gi3/13
Router(config-if)#
spanning-tree mst simulate pvst disable
Router(config-if)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree port-priority	Sets an interface priority when two bridges vie for position as the root bridge.

spanning-tree mst simulate pvst global

To enable Per-VLAN Spanning Tree (PVST) simulation globally, enter the **spanning-treemstsimulatepvstglobal**command in global configuration mode. To disable PVST simulation globally, enter the **no**form of this command.

spanning-tree mst simulate pvst global
no spanning-tree mst simulate pvst global

Syntax Description

This command has no arguments or keywords.

Command Default

PVST simulation is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXI	Support for this command was introduced.

Usage Guidelines

PVST simulation is enabled by default so that all interfaces on the device interoperate between Multiple Spanning Tree (MST) and Rapid Per-VLAN Spanning Tree Plus (PVST+). To prevent an accidental connection to a device that does not run MST as the default Spanning Tree Protocol (STP) mode, you can disable PVST simulation. If you disable PVST simulation, the MST-enabled port moves to the blocking state once it detects it is connected to a Rapid PVST+-enabled port. This port remains in the inconsistent state until the port stops receiving Bridge Protocol Data Units (BPDUs), and then the port resumes the normal STP transition process.

To override the global PVST simulation setting for a port, enter the **spanning-treemstsimulatepvst** interface command in the interface command mode.

Examples

This example shows how to prevent the switch from automatically interoperating with a connecting device that is running Rapid PVST+:

```
Router(config)#
no spanning-tree mst simulate pvst global
Router(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree mst simulate pvst (interface)	Overrides the global PVST simulation setting for a port.

spanning-tree pathcost method

To set the default path-cost calculation method, use the **s**panning-tree pathcost method command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree pathcost method {**long** | **short**}
no spanning-tree pathcost method

Syntax Description

long	Specifies the 32-bit based values for default port-path costs.
short	Specifies the 16-bit based values for default port-path costs.

Command Default

short

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command applies to all the spanning-tree instances on the Cisco 7600 series router.

The **long** path-cost calculation method utilizes all 32 bits for path-cost calculation and yields values in the range of 1 through 200,000,000.

The **short** path-cost calculation method (16 bits) yields values in the range of 1 through 65535.

Examples

This example shows how to set the default path-cost calculation method to long:

```
Router(config
#) spanning-tree pathcost method long
Router(config
#)
```

This example shows how to set the default path-cost calculation method to short:

```
Router(config
#) spanning-tree pathcost method short
Router(config
#)
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

spanning-tree portfast (interface)

To enable PortFast mode where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire, use the **spanning-treeportfast** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree portfast
spanning-tree portfast {**disable** | **edge** [**trunk**] | **network** | **trunk**}
no spanning-tree portfast

Syntax Description

disable	Disables PortFast on the interface.
edge	Enables PortFast edge mode on the interface.
network	Enables PortFast network mode on the interface.
trunk	Enables PortFast on the interface even in the trunk mode.

Command Default

The settings that are configured by the **spanning-treeportfastdefault** command.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	Added edge [trunk] and network keywords.

Usage Guidelines

You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the Cisco 7600 series router and network operation.

An interface with PortFast mode enabled is moved directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-time delay.

Be careful when using the **nospanning-treeportfast** command. This command does not disable PortFast if the **spanning-treeportfastdefault** command is enabled.

This command has these states:

- **spanning-tree portfast** --This command enables PortFast unconditionally on the given port.
- **spanning-tree portfast disable** --This command explicitly disables PortFast for the given port. The configuration line shows up in the running configuration because it is not the default.
- **spanning-tree portfast edge** --This command allows you to configure PortFast edge mode on the given port.
- **spanning-tree portfast network** --This command allows you to configure PortFast network mode on the given port.

- **spanning-tree portfast** [**edge**] **trunk**--This command allows you to configure PortFast on trunk ports. The **edge**keyword is required with **trunk**in Cisco IOS Release 12.2(33)SXI and later releases.

Note If you enter the **spanning-treeportfasttrunk** command, th e port is configured for PortFast even in the access mode.

- **no spanning-tree portfast** --This command implicitly enables PortFast if you define the **spanning-treeportfastdefault** command in global configuration mode and if the port is not a trunk port. If you do not configure PortFast globally, the **nospanning-treeportfast** command is equivalent to the **spanning-treeportfastdisable** command.

Examples

This example shows how to enable PortFast mode in releases earlier than Cisco IOS Release 12.2(33)SXI:

```
Router(config-if)#
spanning-tree portfast
Router(config-if)#
```

This example shows how to enable PortFast edge mode in Cisco IOS Release 12.2(33)SXI and later releases:

```
Router(config-if)#
spanning-tree portfast edge
Router(config-if)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree portfast default	Enables PortFast by default on all access ports.

spanning-tree portfast bpduguard default

To enable bridge protocol data unit (BPDU) guard by default on all PortFast ports, use the **spanning-treeportfastbpduguarddefault**command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree portfast bpduguard default
no spanning-tree portfast bpduguard default

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Caution Be careful when using this command. You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the Cisco 7600 series router and network operation.

BPDU guard disables a port if it receives a BPDU. BPDU guard is applied only on ports that are PortFast enabled and are in an operational PortFast state.

Examples

This example shows how to enable BPDU guard by default:

```
Router(config)#
spanning-tree portfast bpduguard default
Router(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree bpdufilter	Enables BPDU filtering on the interface.

spanning-tree portfast default

To enable PortFast by default on all access ports, use the **spanning-treeportfastdefault**command in global configuration mode. To disable PortFast by default on all access ports, use the **no** form of this command.

spanning-tree portfast {**edge** [{**bpdufilter** | **bpduguard**}] | **network** | **normal**} **default**
no spanning-tree portfast {**edge** [{**bpdufilter** | **bpduguard**}] | **network** | **normal**} **default**

Syntax Description

bpdufilter	Enables PortFast edge BPDU filter by default on all PortFast edge ports.
bpduguard	Enables PortFast edge BPDU guard by default on all PortFast edge ports.
edge	Enables PortFast edge mode by default on all switch access ports.
network	Enables PortFast network mode by default on all switch access ports.
normal	Enables PortFast normal mode by default on all switch access ports.

Note These keywords are available only in Cisco IOS Release 12.2(33)SXI and later releases.

Command Default

PortFast is disabled by default on all access ports.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	Mode settings (edge, network, and normal) and BPDU filter and BPDU guard settings were added.

Usage Guidelines

Caution Be careful when using this command. You should use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the operation of the router or switch and the network.

An interface with PortFast mode enabled is moved directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-time delay.

You can enable PortFast mode on individual interfaces using the **spanning-treeportfast** (interface) command.

Examples

This example shows how to enable PortFast by default on all access ports in releases earlier than Cisco IOS Release 12.2(33)SXI:

```
Router(config)#
spanning-tree portfast default
Router(config)#
```

This example shows how to enable PortFast edge mode with BPDU Guard by default on all access ports in Cisco IOS Release 12.2(33)SXI and later releases:

```
Router(config)#
spanning-tree portfast edge bpduguard default
Router(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree portfast (interface)	Enables PortFast on a specific interface.

spanning-tree port-priority

To set an interface priority when two bridges tie for position as the root bridge, use the **spanning-treeport-priority** command in interface configuration and template configuration mode. To revert to the default value, use the **no** form of this command.

spanning-tree port-priority *port-priority*
no spanning-tree port-priority

Syntax Description

port-priority -	Port priority; valid values are from 2 to 255. The default is 128. **Note** When configuring port priority using an interface template, the range is from 0 to 240 in increments of 16.

Command Default

The default port priority is 128.

Command Modes

Interface configuration (config-if)

Template configuration (config-if)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.2(2)E	This command was integrated into Cisco IOS Release 15.2(2)E. This command is supported in template configuration mode.
Cisco IOS XE Release 3.6E	This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.

Usage Guidelines

The priority you set breaks the tie between two bridges to be designated as a root bridge.

Examples

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:

```
Router(config)# interface ethernet 2/0
Router(config-if)# spanning-tree port-priority 20
Router(config-if)#
```

The following example shows how increase the likelihood that spanning-tree instance 20 is chosen as the root-bridge on an interface using an interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# spanning-tree port-priority 20
Device(config-template)# end
```

Related Commands

Command	Description
show spanning -tree	Displays spanning-tree information for the specified spanning-tree instances.
spanning -treecost	Sets the path cost of the interface for STP calculations.
spanning-tree mst	Sets the path cost and port-priority parameters for any MST instance (including the CIST with instance ID 0).
spanning-tree portfast (global)	Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire.
spanning-tree portfast (interface)	Enables PortFast mode, which places the interface immediately into the forwarding state upon linkup without waiting for the timer to expire.
spanning -treeuplinkfast	Enables the UplinkFast feature.
spanning -treevlan	Configures STP on a per-VLAN basis.

spanning-tree transmit hold-count

To specify the transmit hold count, use the **spanning-treetransmithold-count** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree transmit hold-count *value*
no spanning-tree transmit hold-count

Syntax Description

value	Number of bridge protocol data units (BPDUs) that can be sent before pausing for 1 second; valid values are from 1 to 20.

Command Default

value is **6**

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on all spanning-tree modes.

The transmit hold count determines the number of BPDUs that can be sent before pausing for 1 second.

Note Changing this parameter to a higher value may have a significant impact on CPU utilization, especially in rapid-Per-VLAN Spanning Tree (PVST) mode. Lowering this parameter could slow convergence in some scenarios. We recommend that you do not change the value from the default setting.

If you change the *value* setting, enter the **showrunning-config** command to verify the change.

If you delete the command, use the **showspanning-treemst**command to verify the deletion.

Examples

This example shows how to specify the transmit hold count:

```
Router(config)# spanning-tree transmit hold-count 8
Router(config)#
```

Related Commands

Command	Description
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.
show spanning-tree mst	Display the information about the MST protocol.

spanning-tree uplinkfast

To enable UplinkFast, use the **spanning-treeuplinkfast** command in global configuration mode. To disable UplinkFast, use the **no** form of this command.

spanning-tree uplinkfast [**max-update-rate** *packets-per-second*]
no spanning-tree uplinkfast [**max-update-rate**]

Syntax Description

max-update-rate *packets-per-second*	(Optional) Specifies the maximum rate (in packets per second) at which update packets are sent; valid values are from 0 to 65535.

Command Default

The defaults are as follows:

- UplinkFast is disabled.
- *packets-per-second* is 150 packets per second.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command only on access switches.

When you configure UplinkFast, the bridge priority is changed to 49152 so that this switch is not selected as root. All interface path costs of all spanning-tree interfaces that belong to the specified spanning-tree instances also increase by 3000.

When spanning tree detects that the root interface has failed, UplinkFast causes an immediate switchover to an alternate root interface, transitioning the new root interface directly to the forwarding state. During this time, a topology change notification is sent. To minimize the disruption that is caused by the topology change, a multicast packet is sent to 01-00-0C-CD-CD-CD for each station address in the forwarding bridge except for those associated with the old root interface.

Use the **spanning-treeuplinkfastmax-update-rate** command to enable UplinkFast (if it is not already enabled) and change the rate at which update packets are sent. Use the **no** form of this command to return to the default rate.

Examples

This example shows how to enable UplinkFast and set the maximum rate to 200 packets per second:

```
Router(config)#
 spanning-tree uplinkfast max-update-rate 200
Router(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

spanning-tree vlan

To configure Spanning Tree Protocol (STP) on a per-virtual LAN (VLAN) basis, use the **spanning-treevlan** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree vlan *vlan-id* [{**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds* | **priority** *priority* | **protocol** *protocol* | [**root** {**primary** | **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]]}]
no spanning-tree vlan *vlan-id* [{**forward-time** | **hello-time** | **max-age** | **priority** | **protocol** | **root**}]

Syntax Description

vlan id	VLAN identification number; valid values are from 1 to 1005. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094.
forward -time*seconds*	(Optional) Sets the STP forward delay time; valid values are from 4 to 30 seconds.
hello -time*seconds*	(Optional) Specifies the duration, in seconds, between the generation of configuration messages by the root switch; valid values are from 1 to 10 seconds.
max -age*seconds*	(Optional) Sets the maximum number of seconds the information in a bridge packet data unit (BPDU) is valid; valid values are from 6 to 40 seconds.
priority *priority*	(Optional) Sets the STP bridge priority; valid values are from 0 to 65535.
protocol *protocol*	(Optional) Sets the STP. See the "Usage Guidelines" section for a list of valid values.
root primary	(Optional) Forces this switch to be the root bridge.
root secondary	(Optional) Specifies this switch to act as the root switch should the primary root fail.
diameter *net -diameter*	(Optional) Specifies the maximum number of bridges between any two points of attachment of end stations; valid values are from 2 through 7.

Command Default

The defaults are:

- **forward-time** --15 seconds
- **hello-time** --2 seconds
- **max-age** --20 seconds
- **priority** --The default with IEEE STP enabled is 32768; the default with STP enabled is 128.
- **protocol** --IEEE
- **root** --No STP root

When you issue the **nospanning-treevlan***xx***root** command the following parameters are reset to their defaults:

- **priority** --The default with IEEE STP enabled is 32768; the default with STP enabled is 128.
- **hello-time** --2 seconds

- **forward-time** --15 seconds
- **max-age** --20 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.1(1)E	Support for this command on the Catalyst 6000 series switches was extended to Cisco IOS Release 12.1(1)E.
12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	This command was modified to extend the range of valid VLAN IDs to 1-4094 for specified platforms.

Usage Guidelines

Caution When disabling spanning tree on a VLAN using the no spanning-tree vlan *vlan-id* command, ensure that all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the same VLAN because switches and bridges with spanning tree enabled have incomplete information about the physical topology of the network.

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

When you set the **max-age***seconds* parameter, if a bridge does not hear bridge protocol data units (BPDUs) from the root bridge within the specified interval, it assumes that the network has changed and recomputes the spanning-tree topology.

Valid values for *protocol* are **dec** (Digital STP), **ibm** (IBM STP), **ieee** (IEEE Ethernet STP), and **vlan-bridge** (VLAN Bridge STP).

The **spanning-treerootprimary** command alters this switch’s bridge priority to 8192. If you enter the **spanning-treerootprimary** command and the switch does not become the root switch, then the bridge priority is changed to 100 less than the bridge priority of the current bridge. If the switch still does not become the root, an error results.

The **spanningtreerootsecondary**command alters this switch’s bridge priority to 16384. If the root switch should fail, this switch becomes the next root switch.

Use the **spanningtreeroot** commands on backbone switches only.

The **spanning-treeetherchannelguardmisconfig** command detects two types of errors: misconfiguration and misconnection errors. A misconfiguration error is an error between the port-channel and an individual port. A misconnection error is an error between a switch that is channeling more ports and a switch that is not using enough Spanning Tree Protocol (STP) Bridge Protocol Data Units (BPDUs) to detect the error. In this case, the switch will only error disable an EtherChannel if the switch is a nonroot switch.

Examples

The following example shows how to enable spanning tree on VLAN 200:

```
Router(config)# spanning-tree vlan 200
```

The following example shows how to configure the switch as the root switch for VLAN 10 with a network diameter of 4:

```
Router(config)# spanning-tree vlan 10 root primary diameter 4
```

The following example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
Router(config)# spanning-tree vlan 10 root secondary diameter 4
```

Related Commands

Command	Description
spanning -treecost	Sets the path cost of the interface for STP calculations.
spanning-tree etherchannel guard misconfig	Displays an error message when a loop due to a channel misconfiguration is detected
spanning -treeport-priority	Sets an interface priority when two bridges tie for position as the root bridge.
spanning -treeportfast(global)	Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup, without waiting for the timer to expire.
spanning-tree portfast (interface)	Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup, without waiting for the timer to expire.
spanning -treeuplinkfast	Enables the UplinkFast feature.
show spanning -tree	Displays spanning-tree information for the specified spanning-tree instances.

storm-control

To enable broadcast, multicast, or unicast storm control on a port or to specify the action when a storm occurs on a port, use the **storm-control** command in interface configuration mode. To disable storm control for broadcast, multicast, or unicast traffic or to disable the specified storm-control action, use the **no** form of this command.

storm-control {{**broadcast** | **multicast** | **unicast**} **level** *level* | **action** {**shutdown** | **trap**}}
no storm-control {{**broadcast** | **multicast** | **unicast**} **level** | **action** {**shutdown** | **trap**}}

Cisco ME 2600X Series Ethernet Access Switch
storm-control {{**broadcast** | **multicast**} **cir** *cir-value* | **action shutdown**}
no storm-control {{**broadcast** | **multicast**} **cir** *cir-value* | **action shutdown**}

Syntax Description

broadcast	Enables broadcast storm control on the port.
multicast	Enables multicast storm control on the port.
unicast	Enables unicast storm control on the port.
level *level*	Defines the rising and falling suppression levels. • *level* —Rising suppression level as a percent of the total bandwidth (up to two decimal places). The valid values are from 0 to 100. When the value specified for a level is reached, the flooding of storm packets is blocked.
action	Specifies the action to take when a storm occurs on a port. The default action is to filter traffic.
shutdown	Disables the port during a storm.
trap	Sends a Simple Network Management Protocol (SNMP) trap.
cir *cir-value*	Defines the Committed Information Rate (cir). • *cir-value*—The acceptable range is 10000000 -1000000000 for a gigabit ethernet interface, and 100000000-10000000000 for a ten gigabit interface. The recommended maximum value is up to 98 percent.

Command Default

Broadcast, multicast, and unicast storm control is disabled. The default action is to filter traffic.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(2)XT	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support switchport creation.

Release	Modification
12.2(15)ZJ	This command was integrated into Cisco IOS Release 12.2(15)ZJ. The **level** *level* keyword-argument pair, and the **action** and **shutdown** keywords were added.
15.0(1)S	This command was modified. The **trap** keyword was added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.2(02)SA	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

Use the **storm-control** command to enable or disable broadcast, multicast, or unicast storm control on a port. After a port is disabled during a storm, use the **no shutdown** interface configuration command to enable the port.

The suppression levels are entered as a percentage of total bandwidth. A suppression value of 100 percent means that no limit is placed on the specified traffic type. This command is enabled only when the rising suppression level is less than 100 percent. If no other storm-control configuration is specified, the default action is to filter the traffic that is causing the storm.

When a storm occurs and the action is to filter traffic, and the falling suppression level is not specified, the networking device blocks all traffic until the traffic rate drops below the rising suppression level. If the falling suppression level is specified, the networking device blocks traffic until the traffic rate drops below this level.

When a multicast or unicast storm occurs and the action is to filter traffic, the networking device blocks all traffic (broadcast, multicast, and unicast traffic) and sends only Spanning Tree Protocol (STP) packets.

When a broadcast storm occurs and the action is to filter traffic, the networking device blocks only broadcast traffic.

The trap action is used to send an SNMP trap when a broadcast storm occurs.

Note Adding or removing of storm control configuration under the member link of LACP is not supported.

Note On Cisco Catalyst 3750 Series Switches, when the **storm-control** command is applied, it is rejected and the port is not put into a suspended state.

Examples

The following example shows how to enable broadcast storm control on a port with a 75.67-percent rising suppression level:

```
Device(config-if)# storm-control broadcast level 75.67
```

The following example shows how to enable multicast storm control on a port with an 87-percent rising suppression level:

```
Device(config-if)# storm-control multicast level 87
```

The following example shows how to enable the shutdown action on a port:

```
Device(config-if)# storm-control action shutdown
```

The following example shows how to disable the shutdown action on a port:

```
Device(config-if)# no storm-control action shutdown
```

The following example shows how to enable the trap action on a port:

```
Device(config-if)# storm-control action trap
```

The following example shows how to disable the trap action on a port:

```
Device(config-if)# no storm-control action trap
```

Related Commands

Command	Description
no shutdown	Enables a port.
show storm-control	Displays the packet-storm control information.
shutdown (interface)	Disables an interface.