

traceroute mac

Use the **traceroute mac** privileged EXEC command to display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.

```
traceroute mac [interface interface-id] {source-mac-address} [interface interface-id]
                 {destination-mac-address} [vlan vlan-id] [detail]
```

Syntax Description		
interface <i>interface-id</i>	(Optional) Specify an interface on the source or destination switch.	
<i>source-mac-address</i>	Specify the MAC address of the source switch in hexadecimal format.	
<i>destination-mac-address</i>	Specify the MAC address of the destination switch in hexadecimal format.	
vlan <i>vlan-id</i>	(Optional) Specify the VLAN on which to trace the Layer 2 path that the packets take from the source switch to the destination switch. The range is 1 to 4094.	
detail	(Optional) Specify that detailed information appears.	

Defaults There is no default.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(12c)EA1	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.

When the switch detects a device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and an error message appears.

The **traceroute mac** command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN. If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.

If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination MAC addresses:

```
Switch# tracert mac 0000.0201.0601 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 (2.2.6.6) :Fa0/1 => Fa0/3
con5          (2.2.5.5) ) : Fa0/3 => Gi0/1
con1          (2.2.1.1) ) : Gi0/1 => Gi0/2
con2          (2.2.2.2) ) : Gi0/2 => Fa0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows how to display the Layer 2 path by using the **detail** keyword:

```
Switch# tracert mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C2950G-24-EI / 2.2.6.6 :
    Fa0/1 [auto, auto] => Fa0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
    Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination switches:

```
Switch# tracert mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 (2.2.6.6) :Fa0/1 => Fa0/3
con5          (2.2.5.5) ) : Fa0/3 => Gi0/1
con1          (2.2.1.1) ) : Gi0/1 => Gi0/2
con2          (2.2.2.2) ) : Gi0/2 => Fa0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows the Layer 2 path when the switch is not connected to the source switch:

```
Switch# tracert mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source ....
Source 0000.0201.0501 found on con5[WS-C2950G-24-EI] (2.2.5.5)
con5 / WS-C2950G-24-EI / 2.2.5.5 :
    Fa0/1 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows the Layer 2 path when the switch cannot find the destination port for the source MAC address:

```
Switch# tracert mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
```

This example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace aborted.
```

This example shows the Layer 2 path when the destination MAC address is a multicast address:

```
Switch# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```

This example shows the Layer 2 path when source and destination switches belong to multiple VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

Related Commands

Command	Description
traceroute mac ip	Displays the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname.

tracertoute mac ip

Use the **tracertoute mac** privileged EXEC command to display the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname.

```
tracertoute mac ip {source-ip-address | source-hostname} {destination-ip-address | destination-hostname} [detail]
```

Syntax Description

<i>source-ip-address</i>	Specify the IP address of the source switch as a 32-bit quantity in dotted-decimal format.
<i>destination-ip-address</i>	Specify the IP address of the destination switch as a 32-bit quantity in dotted-decimal format.
<i>source-hostname</i>	Specify the IP hostname of the source switch.
<i>destination-hostname</i>	Specify the IP hostname of the destination switch.
detail	(Optional) Specify that detailed information appears.

Defaults

There is no default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(12c)EA1	This command was introduced.

Usage Guidelines

For Layer 2 tracertoute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.

When the switch detects an device in the Layer 2 path that does not support Layer 2 tracertoute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The **tracertoute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet. When you specify the IP addresses, the switch uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

- If an ARP entry exists for the specified IP address, the switch uses the associated MAC address and identifies the physical path.
- If an ARP entry does not exist, the switch sends an ARP query and tries to resolve the IP address. The IP addresses must be in the same subnet. If the IP address is not resolved, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the **detail** keyword:

```
Switch# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C2950G-24-EI / 2.2.6.6 :
      Fa0/1 [auto, auto] => Fa0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
      Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
      Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
      Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Switch# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Fa0/1 => Fa0/3
con5          (2.2.5.5       ) :   Fa0/3 => Gi0/1
con1          (2.2.1.1       ) :   Gi0/1 => Gi0/2
con2          (2.2.2.2       ) :   Gi0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

This example shows the Layer 2 path when ARP cannot associate the source IP address with the corresponding MAC address:

```
Switch# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

Related Commands

Command	Description
traceroute mac	Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.

trust

Use the **trust** policy-map class configuration command to define a trust state for traffic classified by the **class** or the **class-map** command. Use the **no** form of this command to return to the default setting.

trust [**cos** | **dscp** | **ip-precedence**]

no trust [**cos** | **dscp** | **ip-precedence**]

Syntax Description

cos	(Optional) Classify ingress packets by using the packet class of service (CoS) values. For untagged packets, the port default CoS value is used.
dscp	(Optional) Classify ingress packets by using the packet Differentiated Services Code Point (DSCP) values (most significant 6 bits of 8-bit service-type field). For non-IP packets, the packet CoS value is used if the packet is tagged. If the packet is untagged, the default port CoS value is used to map CoS to DSCP.
ip-precedence	(Optional) Classify ingress packets by using the packet IP-precedence values (most significant 3 bits of 8-bit service-type field). For non-IP packets, the packet CoS value is used if the packet is tagged. If the packet is untagged, the port default CoS value is used to map CoS to DSCP.

Defaults

The action is not trusted. If no keyword is specified when the command is entered, the default is **dscp**.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

Use this command to distinguish the quality of service (QoS) trust behavior for certain traffic from others. For example, incoming traffic with certain DSCP values can be trusted. You can configure a class map to match and trust the DSCP values in the incoming traffic.

Trust values set with this command supersede trust values set on specific interfaces with the **mls qos trust** interface configuration command.

The **trust** command is mutually exclusive with **set** policy-map class configuration command within the same policy map.

You cannot use the **service-policy** interface configuration command to attach policy maps that contain these elements to an egress interface:

- **set** or **trust** policy-map class configuration commands. Instead, you can use the **police** policy-map class configuration command to mark down (reduce) the DSCP value at the egress interface.
- Access control list (ACL) classification.
- Per-port per-VLAN classification.

The only match criterion in a policy map that can be attached to an egress interface is the **match ip dscp dscp-list** class-map configuration command.

If you specify **trust cos**, QoS derives the internal DSCP value by using the received or default port CoS value and the CoS-to-DSCP map.

If you specify **trust dscp**, QoS derives the internal DSCP value by using the DSCP value from the ingress packet. For non-IP packets that are tagged, QoS derives the internal DSCP value by using the received CoS value; for non-IP packets that are untagged, QoS derives the internal DSCP value by using the default port CoS value. In either case, the internal DSCP value is derived from the CoS-to-DSCP map.

If you specify **trust ip-precedence**, QoS derives the internal DSCP value by using the IP precedence value from the ingress packet and the IP-precedence-to-DSCP map. For non-IP packets that are tagged, QoS derives the internal DSCP value by using the received CoS value; for non-IP packets that are untagged, QoS derives the internal DSCP value by using the default port CoS value. In either case, the internal DSCP value is derived from the CoS-to-DSCP map.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Examples

This example shows how to define a port trust state to trust incoming DSCP values for traffic classified with *class1*:

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Related Commands

Command	Description
class	Defines a traffic classification for the policy to act on.
police	Defines a policer for classified traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple interfaces to specify a service policy.
show policy-map	Displays QoS policy maps.

udld

Use the **udld** global configuration command to enable aggressive or normal mode in the UniDirectional Link Detection (UDLD) and to set the configurable message timer time. Use the **no** form of this command to disable aggressive or normal mode UDLD on all fiber-optic ports.

udld { **aggressive** | **enable** | **message time** *message-timer-interval* }

no udld { **aggressive** | **enable** | **message** }

Syntax Description

aggressive	Enable UDLD in aggressive mode on all fiber-optic interfaces.
enable	Enable UDLD in normal mode on all fiber-optic interfaces.
message time <i>message-timer-interval</i>	Configure the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is 1 to 90 seconds.

Defaults

UDLD is disabled on all fiber-optic interfaces.
The message timer is set at 60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.2(25)SEC	The range for <i>message-timer-interval</i> was changed from 7 to 90 seconds to 1 to 90 seconds.

Usage Guidelines

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about normal and aggressive modes, see the “Understanding UDLD” section in the software configuration guide for this release.

If you change the message time between probe packets, you are making a trade-off between the detection speed and the CPU load. By decreasing the time, you can make the detection-response faster but increase the load on the CPU.

This command affects fiber-optic interfaces only. Use the **udld** interface configuration command to enable UDLD on other interface types.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command to reset all interfaces shut down by UDLD
- The **shutdown** and **no shutdown** interface configuration commands
- The **no udld enable** global configuration command followed by the **udld {aggressive | enable}** global configuration command to re-enable UDLD globally. The **udld port disable** interface configuration command followed by the **udld port** or **udld port aggressive** interface configuration command to re-enable UDLD on the specified interface
- The **errdisable recovery cause udld** and **errdisable recovery interval *interval*** global configuration commands to automatically recover from the UDLD error-disabled state

Examples

This example shows how to enable UDLD on all fiber-optic interfaces:

```
Switch(config)# udld enable
```

You can verify your setting by entering the **show udld** privileged EXEC command.

Related Commands

Command	Description
show udld	Displays UDLD administrative and operational status for all ports or the specified port.
udld port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the udld global configuration command.
udld reset	Resets all interfaces shut down by UDLD and permits traffic to again pass through.

uddl port

Use the **uddl port** interface configuration command to enable the UniDirectional Link Detection (UDLD) on an individual interface or prevent a fiber-optic interface from being enabled by the **uddl** global configuration command. Use the **no** form of this command to return to the **uddl** global configuration command setting or to disable UDLD if entered for a nonfiber-optic port.

uddl port [aggressive]

no uddl port [aggressive]

Syntax Description

aggressive (Optional) Enable UDLD in aggressive mode on the specified interface.

Defaults

On fiber-optic interfaces, UDLD is neither enabled, not in aggressive mode, and not disabled. For this reason, fiber-optic interfaces enable UDLD according to the state of the **uddl enable** or **uddl aggressive** global configuration command.

On nonfiber-optic interfaces, UDLD is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(14)EA1	The port keyword was added. The enable keyword was removed.
12.1(20)EA2	The disable keyword was removed.

Usage Guidelines

A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch.

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about normal and aggressive modes, see the “Configuring UDLD” chapter in the software configuration guide for this release.

To enable UDLD in normal mode, use the **uddl port** interface configuration command. To enable UDLD in aggressive mode, use the **uddl port aggressive** interface configuration command.

Use the **no uddl port** command on fiber-optic ports to return control of UDLD to the **uddl enable** global configuration command or to disable UDLD on nonfiber-optic ports.

Use the **uddl port aggressive** command on fiber-optic ports to override the setting of the **uddl enable** or **uddl aggressive** global configuration command. Use the **no** form on fiber-optic ports to remove this setting and to return control of UDLD enabling to the **uddl** global configuration command or to disable UDLD on nonfiber-optic ports.

If the switch software detects a Gigabit Interface Converter (GBIC) module change and the port changes from fiber optic to nonfiber optic or vice versa, all configurations are maintained.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command to reset all interfaces shut down by UDLD
- The **shutdown** and **no shutdown** interface configuration commands
- The **no udld enable** global configuration command followed by the **udld {aggressive | enable}** global configuration command to re-enable UDLD globally
- The **no udld port** interface configuration command followed by the **udld port** or **udld port aggressive** interface configuration command to re-enable UDLD on the specified interface
- The **errdisable recovery cause udld** and **errdisable recovery interval interval** global configuration commands to automatically recover from the UDLD error-disabled state

Examples

This example shows how to enable UDLD on an interface:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# udld port
```

This example shows how to disable UDLD on a fiber-optic interface despite the setting of the **udld** global configuration command:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no udld port
```

You can verify your settings by entering the **show running-config** or the **show udld interface** privileged EXEC command.

Related Commands

Command	Description
show running-config	Displays the running configuration on the switch. For syntax information, for more information about configuring an SDM template Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands.
show udld	Displays UDLD administrative and operational status for all ports or the specified port.
udld	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udld reset	Resets all interfaces shut down by UDLD and permits traffic to again pass through.

udd reset

Use the **udd reset** privileged EXEC command to reset all interfaces shutdown by the UniDirectional Link Detection (UDLD) and permit traffic to begin passing through them again (though other features, such as spanning tree, Port Aggregation Protocol (PAgP), and Dynamic Trunking Protocol (DTP) still have their normal effects, if enabled).

udd reset

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(4)EA1	This command was introduced.

Usage Guidelines If the interface configuration is still enabled for UDLD, these ports begin to run UDLD again and might shutdown for the same reason if the problem has not been corrected.

Examples This example shows how to reset all interfaces disabled by UDLD:

```
Switch# udd reset
1 ports shutdown by UDLD were reset.
```

You can verify your setting by entering the **show udd** privileged EXEC command.

Related Commands	Command	Description
	show running-config	Displays the running configuration on the switch. For syntax information, for more information about configuring an SDM template Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands.
	show udd	Displays UDLD administrative and operational status for all ports or the specified port.
	udd	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
	udd port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the udd global configuration command.

vlan (global configuration)

Use the **vlan** global configuration command to add a VLAN and enter the config-vlan mode. Use the **no** form of this command to delete the VLAN.

vlan *vlan-id*

no vlan *vlan-id*

Syntax Description	<i>vlan-id</i>	ID of the VLAN to be added and configured. The range is 1 to 4094; do not enter leading zeros. You can enter a single VLAN ID, a series of VLAN IDs separated by commas, or a range of VLAN IDs separated by hyphens.
---------------------------	----------------	---

Defaults	This command has no default settings.
-----------------	---------------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.1(9)EA1	This command was introduced.
	12.1(11)EA1	The remote-span configuration command was added.

Usage Guidelines

You must use the **vlan** *vlan-id* global configuration command to add extended-range VLANs (VLAN IDs 1006 to 4094). Before configuring VLANs in the extended range, you must use the **vtp transparent** global configuration or VLAN configuration command to put the switch in VTP transparent mode. Extended-range VLANs are not learned by VTP and are not added to the VLAN database, but when VTP mode is transparent, VTP mode and domain name and all VLAN configurations are saved in the running configuration, and you can save them in the switch startup configuration file by entering the **copy running-config startup-config** privileged EXEC command.

When you save the VLAN and VTP configurations in the startup configuration file and reboot the switch, the configuration is determined in these ways:

- If both the VLAN database and the configuration file show the VTP mode as transparent and the VTP domain names match, the VLAN database is ignored. The VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode is server, or if the startup VTP mode or domain names do not match the VLAN database, the VTP mode and the VLAN configuration for the first 1005 VLANs use the VLAN database information.
- If the image on the switch or the configuration file is earlier than Cisco IOS Release 12.1(9)EA1, the switch reboots with information in the VLAN database.

Configuration information for normal-range VLANs (VLAN IDs 1 to 1005) is always saved in the VLAN database.

If you try to create an extended-range VLAN when the switch is not in VTP transparent mode, the VLAN is rejected, and you receive an error message.

If you enter an invalid VLAN ID, you receive an error message and do not enter config-vlan mode.

Entering the **vlan** command with a VLAN ID enables config-vlan mode. When you enter the VLAN ID of an existing VLAN, you do not create a new VLAN, but you can modify VLAN parameters for that VLAN. The specified VLANs are added or modified when you exit the config-vlan mode. Only the **shutdown** command (for VLANs 1 to 1005) takes effect immediately.

These configuration commands are available in config-vlan mode. The **no** form of each command returns the characteristic to its default state.


Note

Although all commands are visible, the only config-vlan command supported on extended-range VLANs is **mtu** *mtu-size*. For extended-range VLANs, all other characteristics must remain at the default state.

- **are** *are-number*: defines the maximum number of all-routes explorer (ARE) hops for this VLAN. This keyword applies only to TrCRF VLANs. The range is 0 to 13. The default is 7. If no value is entered, 0 is assumed to be the maximum.
- **backupcrf**: specifies the backup CRF mode. This keyword applies only to TrCRF VLANs.
 - **enable** backup CRF mode for this VLAN.
 - **disable** backup CRF mode for this VLAN (the default).
- **bridge** *{bridge-number| type}*: specifies the logical distributed source-routing bridge, the bridge that interconnects all logical rings having this VLAN as a parent VLAN in FDDI-NET, Token Ring-NET, and TrBRF VLANs. The range is 0 to 15. The default bridge number is 0 (no source-routing bridge) for FDDI-NET, TrBRF, and Token Ring-NET VLANs. The **type** keyword applies only to TrCRF VLANs and is one of these:
 - **srb** (source-route bridging)
 - **srt** (source-route transparent) bridging VLAN
- **exit**: applies changes, increments the VLAN database revision number (VLANs 1 to 1005 only), and exits config-vlan mode.
- **media**: defines the VLAN media type. See [Table 2-31](#) for valid commands and syntax for different media types.


Note

The switch supports only Ethernet ports. You configure only FDDI and Token Ring media-specific characteristics for VLAN Trunking Protocol (VTP) global advertisements to other switches. These VLANs are locally suspended.

- **ethernet** is Ethernet media type (the default).
- **fddi** is FDDI media type.
- **fd-net** is FDDI network entity title (NET) media type.
- **tokenring** is Token Ring media type if the VTP v2 mode is disabled, or TrCRF if the VTP version 2 (v) mode is enabled.
- **tr-net** is Token Ring network entity title (NET) media type if the VTP v2 mode is disabled or TrBRF media type if the VTP v2 mode is enabled.

- **mtu** *mtu-size*: specifies the maximum transmission unit (MTU) (packet size in bytes). The range is 1500 to 18190. The default is 1500 bytes.
- **name** *vlan-name*: names the VLAN with an ASCII string from 1 to 32 characters that must be unique within the administrative domain. The default is *VLANxxxx* where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number.
- **no**: negates a command or returns it to the default setting.
- **parent** *parent-vlan-id*: specifies the parent VLAN of an existing FDDI, Token Ring, or TrCRF VLAN. This parameter identifies the TrBRF to which a TrCRF belongs and is required when defining a TrCRF. The range is 0 to 1005. The default parent VLAN ID is 0 (no parent VLAN) for FDDI and Token Ring VLANs. For both Token Ring and TrCRF VLANs, the parent VLAN ID must already exist in the database and be associated with a Token Ring-NET or TrBRF VLAN.

**Note**

Though visible in the command-line interface, the **private-vlan** command is not supported.

- **remote-span**: adds the Remote SPAN (RSPAN) feature to the VLAN. When the RSPAN feature is added to an existing VLAN, the VLAN is first deleted and is then recreated with the RSPAN feature. Any access ports are deactivated until the RSPAN feature is removed. The new RSPAN VLAN is propagated by VTP for VLAN-IDs that are lower than 1024. Learning is disabled on the VLAN. Only Layer 2 switch protocols will be processed by the CPU. Broadcast packets, multicast packets and unicast packets addressed directly to the switch will be flooded on the VLAN but will not be forwarded to the CPU.
- **ring** *ring-number*: defines the logical ring for an FDDI, Token Ring, or TrCRF VLAN. The range is 1 to 4095. The default for Token Ring VLANs is 0. For FDDI VLANs, there is no default.
- **said** *said-value*: specifies the security association identifier (SAID) as documented in IEEE 802.10. The range is 1 to 4294967294 and must be unique within the administrative domain. The default value is 100000 plus the VLAN ID number.
- **shutdown**: shuts down VLAN switching on the VLAN. This command takes effect immediately. Other commands take effect when you exit config-vlan mode.
- **state**: specifies the VLAN state:
 - **active** means the VLAN is operational (the default).
 - **suspend** means the VLAN is suspended. Suspended VLANs do not pass packets.
- **ste** *ste-number*: defines the maximum number of spanning-tree explorer (STE) hops. This keyword applies only to TrCRF VLANs. The range is 0 to 13. The default is 7.
- **stp type**: defines the spanning-tree type for FDDI-NET, Token Ring-NET, or TrBRF VLANs. For FDDI-NET VLANs, the default STP type is **ieee**. For Token Ring-NET VLANs, the default STP type is **ibm**. For FDDI and Token Ring VLANs, the default is no type specified.
 - **ieee** for IEEE Ethernet STP running source-route transparent (SRT) bridging.
 - **ibm** for IBM STP running source-route bridging (SRB).
 - **auto** for STP running a combination of source-route transparent bridging (IEEE) and source-route bridging (IBM).
- **tb-vlan1** *tb-vlan1-id* and **tb-vlan2** *tb-vlan2-id*: specifies the first and second VLAN to which this VLAN is translationally bridged. Translational VLANs translate FDDI or Token Ring to Ethernet, for example. The range is 0 to 1005. If no value is specified, 0 (no transitional bridging) is assumed.

Table 2-31 Valid Commands and Syntax for Different Media Types

Media Type	Valid Syntax
Ethernet	name <i>vlan-name</i> , media ethernet , state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , remote-span , tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
FDDI	name <i>vlan-name</i> , media fddi , state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , ring <i>ring-number</i> , parent <i>parent-vlan-id</i> , tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
FDDI-NET	name <i>vlan-name</i> , media fd-net , state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , bridge <i>bridge-number</i> , stp type {ieee ibm auto}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i> If VTP v2 mode is disabled, do not set the stp type to auto .
Token Ring	VTP v1 mode is enabled. name <i>vlan-name</i> , media tokenring , state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , ring <i>ring-number</i> , parent <i>parent-vlan-id</i> , tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
Token Ring concentrator relay function (TrCRF)	VTP v2 mode is enabled. name <i>vlan-name</i> , media tokenring , state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , ring <i>ring-number</i> , parent <i>parent-vlan-id</i> , bridge type {srb srt}, are <i>are-number</i> , ste <i>ste-number</i> , backupcrf {enable disable}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
Token Ring-NET	VTP v1 mode is enabled. name <i>vlan-name</i> , media tr-net , state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , bridge <i>bridge-number</i> , stp type {ieee ibm}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
Token Ring bridge relay function (TrBRF)	VTP v2 mode is enabled. name <i>vlan-name</i> , media tr-net , state {suspend active}, said <i>said-value</i> , mtu <i>mtu-size</i> , bridge <i>bridge-number</i> , stp type {ieee ibm auto}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>

Table 2-32 describes the rules for configuring VLANs.

Table 2-32 VLAN Configuration Rules

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrCRF VLAN media type.	Specify a parent VLAN ID of a TrBRF that already exists in the database. Specify a ring number. Do not leave this field blank. Specify unique ring numbers when TrCRF VLANs have the same parent VLAN ID. Only one backup concentrator relay function (CRF) can be enabled.
VTP v2 mode is enabled, and you are configuring VLANs other than TrCRF media type.	Do not specify a backup CRF.

Table 2-32 VLAN Configuration Rules (continued)

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrBRF VLAN media type.	Specify a bridge number. Do not leave this field blank.
VTP v1 mode is enabled.	No VLAN can have an STP type set to auto. This rule applies to Ethernet, FDDI, FDDI-NET, Token Ring, and Token Ring-NET VLANs.
Add a VLAN that requires translational bridging (values are not set to zero).	The translational bridging VLAN IDs that are used must already exist in the database. The translational bridging VLAN IDs that a configuration points to must also contain a pointer to the original VLAN in one of the translational bridging parameters (for example, Ethernet points to FDDI, and FDDI points to Ethernet). The translational bridging VLAN IDs that a configuration points to must be different media types than the original VLAN (for example, Ethernet can point to Token Ring). If both translational bridging VLAN IDs are configured, these VLANs must be different media types (for example, Ethernet can point to FDDI and Token Ring).

Examples

This example shows how to add an Ethernet VLAN with default media characteristics. The default includes a *vlan-name* of *VLANxxx*, where *xxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number. The default **media** option is **ethernet**; the **state** option is **active**. The default *said-value* variable is 100000 plus the VLAN ID; the *mtu-size* variable is 1500; the **stp-type** option is **ieee**. When you enter the **exit** config-vlan configuration command, the VLAN is added if it did not already exist; otherwise, this command does nothing.

This example shows how to create a new VLAN with all default characteristics and enter config-vlan mode:

```
Switch(config)# vlan 200
Switch(config-vlan)# exit
Switch(config)#
```

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

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

You can verify your setting by entering the **show vlan** privileged EXEC command.

Related Commands	Command	Description
	show running-config vlan	Displays all or a range of VLAN-related configurations on the switch.
	show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.
	vlan (VLAN configuration)	Configures normal-range VLANs in the VLAN database.

vlan (VLAN configuration)

Use the **vlan** VLAN configuration command to configure VLAN characteristics for a normal-range VLAN (VLAN IDs 1 to 1005) in the VLAN database. You access VLAN configuration mode by entering the **vlan database** privileged EXEC command. Use the **no** form of this command without additional parameters to delete a VLAN. Use the **no** form with parameters to change its configured characteristics.

```
vlan vlan-id [are are-number] [backupcrf {enable | disable}] [bridge bridge-number |
type {srb | srt}] [media {ethernet | fddi | fdi-net | tokenring | tr-net}] [mtu mtu-size]
[name vlan-name] [parent parent-vlan-id] [ring ring-number] [said said-value]
[state {suspend | active}] [ste ste-number] [stp type {ieee | ibm | auto}]
[tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]
```

```
no vlan vlan-id [are are-number] [backupcrf {enable | disable}] [bridge bridge-number |
type {srb | srt}] [media {ethernet | fddi | fdi-net | tokenring | tr-net}] [mtu mtu-size]
[name vlan-name] [parent parent-vlan-id] [ring ring-number] [said said-value]
[state {suspend | active}] [ste ste-number] [stp type {ieee | ibm | auto}]
[tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]
```

Extended-range VLANs (with VLAN IDs from 1006 to 4094) cannot be added or modified by using these commands. To add extended-range VLANs, use the **vlan (global configuration)** command to enter config-vlan mode.



Note

The switch supports only Ethernet ports. You configure only FDDI and Token Ring media-specific characteristics for VLAN Trunking Protocol (VTP) global advertisements to other switches. These VLANs are locally suspended.

Syntax Description

<i>vlan-id</i>	ID of the configured VLAN. The range is 1 to 1005 and must be unique within the administrative domain. Do not enter leading zeros.
are <i>are-number</i>	(Optional) Specify the maximum number of all-routes explorer (ARE) hops for this VLAN. This keyword applies only to TrCRF VLANs. The range is 0 to 13. If no value is entered, 0 is assumed to be the maximum.
backupcrf { enable disable }	(Optional) Specify the backup CRF mode. This keyword applies only to TrCRF VLANs. <ul style="list-style-type: none"> enable backup CRF mode for this VLAN. disable backup CRF mode for this VLAN.
bridge <i>bridge-number</i> type { srb srt }	(Optional) Specify the logical distributed source-routing bridge, the bridge that interconnects all logical rings having this VLAN as a parent VLAN in FDDI-NET, Token Ring-NET, and TrBRF VLANs. The range is 0 to 15. The type keyword applies only to TrCRF VLANs and is one of these: <ul style="list-style-type: none"> srb (source-route bridging) srt (source-route transparent) bridging VLAN

media { ethernet fddi fd-net tokenring tr-net }	(Optional) Specify the VLAN media type. Table 2-33 lists the valid syntax for each media type. <ul style="list-style-type: none"> • ethernet is Ethernet media type (the default). • fddi is FDDI media type. • fd-net is FDDI network entity title (NET) media type. • tokenring is Token Ring media type if the VTP v2 mode is disabled, or TrCRF if the VTP v2 mode is enabled. • tr-net is Token Ring network entity title (NET) media type if the VTP v2 mode is disabled or TrBRF media type if the VTP v2 mode is enabled.
mtu <i>mtu-size</i>	(Optional) Specify the maximum transmission unit (MTU) (packet size in bytes). The range is 1500 to 18190.
name <i>vlan-name</i>	(Optional) Specify the VLAN name, an ASCII string from 1 to 32 characters that must be unique within the administrative domain.
parent <i>parent-vlan-id</i>	(Optional) Specify the parent VLAN of an existing FDDI, Token Ring, or TrCRF VLAN. This parameter identifies the TrBRF to which a TrCRF belongs and is required when defining a TrCRF. The range is 0 to 1005.
ring <i>ring-number</i>	(Optional) Specify the logical ring for an FDDI, Token Ring, or TrCRF VLAN. The range is 1 to 4095.
said <i>said-value</i>	(Optional) Enter the security association identifier (SAID) as documented in IEEE 802.10. The range is 1 to 4294967294 and must be unique within the administrative domain.
state { suspend active }	(Optional) Specify the VLAN state: <ul style="list-style-type: none"> • If active, the VLAN is operational. • If suspend, the VLAN is suspended. Suspended VLANs do not pass packets.
ste <i>ste-number</i>	(Optional) Specify the maximum number of spanning-tree explorer (STE) hops. This keyword applies only to TrCRF VLANs. The range is 0 to 13.
stp type { ieee ibm auto }	(Optional) Specify the spanning-tree type for FDDI-NET, Token Ring-NET, or TrBRF VLAN. <ul style="list-style-type: none"> • ieee for IEEE Ethernet STP running source-route transparent (SRT) bridging. • ibm for IBM STP running source-route bridging (SRB). • auto for STP running a combination of source-route transparent bridging (IEEE) and source-route bridging (IBM).
tb-vlan1 <i>tb-vlan1-id</i> and tb-vlan2 <i>tb-vlan2-id</i>	(Optional) Specify the first and second VLAN to which this VLAN is translationally bridged. Translational VLANs translate FDDI or Token Ring to Ethernet, for example. The range is 0 to 1005. Zero is assumed if no value is specified.

[Table 2-33](#) shows the valid syntax options for different media types.

Table 2-33 Valid Syntax for Different Media Types

Media Type	Valid Syntax
Ethernet	vlan <i>vlan-id</i> [name <i>vlan-name</i>] media ethernet [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]
FDDI	vlan <i>vlan-id</i> [name <i>vlan-name</i>] media fddi [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [ring <i>ring-number</i>] [parent <i>parent-vlan-id</i>] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]
FDDI-NET	vlan <i>vlan-id</i> [name <i>vlan-name</i>] media fd-net [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [bridge <i>bridge-number</i>] [stp type { ieee ibm auto }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>] If VTP v2 mode is disabled, do not set the stp type to auto .
Token Ring	VTP v1 mode is enabled. vlan <i>vlan-id</i> [name <i>vlan-name</i>] media tokenring [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [ring <i>ring-number</i>] [parent <i>parent-vlan-id</i>] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]
Token Ring concentrator relay function (TrCRF)	VTP v2 mode is enabled. vlan <i>vlan-id</i> [name <i>vlan-name</i>] media tokenring [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [ring <i>ring-number</i>] [parent <i>parent-vlan-id</i>] [bridge type { srb srt }] [are <i>are-number</i>] [ste <i>ste-number</i>] [backupcrf { enable disable }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]
Token Ring-NET	VTP v1 mode is enabled. vlan <i>vlan-id</i> [name <i>vlan-name</i>] media tr-net [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [bridge <i>bridge-number</i>] [stp type { ieee ibm }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]
Token Ring bridge relay function (TrBRF)	VTP v2 mode is enabled. vlan <i>vlan-id</i> [name <i>vlan-name</i>] media tr-net [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [bridge <i>bridge-number</i>] [stp type { ieee ibm auto }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>]

Table 2-34 describes the rules for configuring VLANs.

Table 2-34 VLAN Configuration Rules

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrCRF VLAN media type.	Specify a parent VLAN ID of a TrBRF that already exists in the database. Specify a ring number. Do not leave this field blank. Specify unique ring numbers when TrCRF VLANs have the same parent VLAN ID. Only one backup concentrator relay function (CRF) can be enabled.
VTP v2 mode is enabled, and you are configuring VLANs other than TrCRF media type.	Do not specify a backup CRF.

Table 2-34 VLAN Configuration Rules (continued)

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrBRF VLAN media type.	Specify a bridge number. Do not leave this field blank.
VTP v1 mode is enabled.	No VLAN can have an STP type set to auto. This rule applies to Ethernet, FDDI, FDDI-NET, Token Ring, and Token Ring-NET VLANs.
Add a VLAN that requires translational bridging (values are not set to zero).	The translational bridging VLAN IDs that are used must already exist in the database. The translational bridging VLAN IDs that a configuration points to must also contain a pointer to the original VLAN in one of the translational bridging parameters (for example, Ethernet points to FDDI, and FDDI points to Ethernet). The translational bridging VLAN IDs that a configuration points to must be different media types than the original VLAN (for example, Ethernet can point to Token Ring). If both translational bridging VLAN IDs are configured, these VLANs must be different media types (for example, Ethernet can point to FDDI and Token Ring).

Defaults

The ARE value is 7.

Backup CRF is disabled.

The bridge number is 0 (no source-routing bridge) for FDDI-NET, TrBRF, and Token Ring-NET VLANs.

The **media** type is **ethernet**.

The default *mtu size* is 1500 bytes.

The *vlan-name* variable is *VLANxxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number.

The parent VLAN ID is 0 (no parent VLAN) for FDDI and Token Ring VLANs. For TrCRF VLANs, you must specify a parent VLAN ID. For both Token Ring and TrCRF VLANs, the parent VLAN ID must already exist in the database and be associated with a Token Ring-NET or TrBRF VLAN.

The *ring number* for Token Ring VLANs is 0. For FDDI VLANs, there is no default.

The *said value* is 100000 plus the VLAN ID.

The state is **active**.

The STE value is 7.

The STP type is **ieec** for FDDI-NET and **ibm** for Token Ring-NET VLANs. For FDDI and Token Ring VLANs, the default is no type specified.

The *tb-vlan1-id* and *tb-vlan2-id* variables are zero (no translational bridging).

Command Modes VLAN configuration

Command History	Release	Modification
	12.1(4)EA1	This command was introduced.
	12.1(13)EA1	The value for <i>vlan-id</i> variable was changed.

Usage Guidelines You can only use this command mode for configuring normal-range VLANs, that is, VLAN IDs 1 to 1005.



Note

To configure extended-range VLANs (VLAN IDs 1006 to 4094), use the **vlan** global configuration command.

VLAN configuration is always saved in the VLAN database. If VTP mode is transparent, it is also saved in the switch running configuration file, along with the VTP mode and domain name. You can then save it in the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

When you save VLAN and VTP configuration in the startup configuration file and reboot the switch, the configuration is determined in these ways:

- If both the VLAN database and the configuration file show the VTP mode as transparent and the VTP domain names match, the VLAN database is ignored. The VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode is server, or if the startup VTP mode or domain names do not match the VLAN database, the VTP mode and the VLAN configuration for the first 1005 VLANs use VLAN database information.
- If the image on the switch or the configuration file is earlier than Cisco IOS Release 12.1(9)EA1, the switch reboots with information in the VLAN database.

The following are the results of using the **no vlan** commands:

- When the **no vlan *vlan-id*** form is used, the VLAN is deleted. Deleting VLANs automatically resets to zero any other parent VLANs and translational bridging parameters that refer to the deleted VLAN.
- When the **no vlan *vlan-id* bridge** form is used, the VLAN source-routing bridge number returns to the default (0). The **vlan *vlan-id* bridge** command is used only for FDDI-NET and Token Ring-NET VLANs and is ignored in other VLAN types.
- When the **no vlan *vlan-id* media** form is used, the media type returns to the default (**ethernet**). Changing the VLAN media type (including the **no** form) resets the VLAN MTU to the default MTU for the type (unless the **mtu** keyword is also present in the command). It also resets the VLAN parent and translational bridging VLAN to the default (unless the **parent**, **tb-vlan1**, or **tb-vlan2** are also present in the command).
- When the **no vlan *vlan-id* mtu** form is used, the VLAN MTU returns to the default for the applicable VLAN media type. You can also modify the MTU by using the **media** keyword.
- When the **no vlan *vlan-id* name *vlan-name*** form is used, the VLAN name returns to the default name (*VLANxxxx*, where *xxxx* represent four numeric digits [including leading zeros] equal to the VLAN ID number).

- When the **no vlan *vlan-id* parent** form is used, the parent VLAN returns to the default (0). The parent VLAN resets to the default if the parent VLAN is deleted or if the **media** keyword changes the VLAN type or the VLAN type of the parent VLAN.
- When the **no vlan *vlan-id* ring** form is used, the VLAN logical ring number returns to the default (0).
- When the **no vlan *vlan-id* said** form is used, the VLAN SAID returns to the default (100,000 plus the VLAN ID).
- When the **no vlan *vlan-id* state** form is used, the VLAN state returns to the default (**active**).
- When the **no vlan *vlan-id* stp type** form is used, the VLAN spanning-tree type returns to the default (**ieee**).
- When the **no vlan *vlan-id* tb-vlan1** or **no vlan *vlan-id* tb-vlan2** form is used, the VLAN translational bridge VLAN (or VLANs, if applicable) returns to the default (0). Translational bridge VLANs must be a different VLAN type than the affected VLAN, and if two are specified, the two must be different VLAN types from each other. A translational bridge VLAN resets to the default if the translational bridge VLAN is deleted, if the **media** keyword changes the VLAN type, or if the **media** keyword changes the VLAN type of the corresponding translation bridge VLAN.

Examples

This example shows how to add an Ethernet VLAN with default media characteristics. The default includes a *vlan-name* of *VLANxxx*, where *xxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number. The default **media** option is **ethernet**; the **state** option is **active**. The default *said-value* variable is 100000 plus the VLAN ID; the *mtu-size* variable is 1500; the **stp-type** option is **ieee**. When you enter the **exit** or **apply** vlan configuration command, the VLAN is added if it did not already exist; otherwise, this command does nothing.

```
Switch(vlan)# vlan 2
VLAN 2 added:
  Name: VLAN0002
Switch(vlan)# exit
APPLY completed.
Exiting...
```

This example shows how to modify an existing VLAN by changing its name and MTU size:

```
Switch(vlan)# no vlan name engineering mtu 1200
```

You can verify your settings by entering the **show vlan** privileged EXEC command.

Related Commands

Command	Description
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.
vlan (global configuration)	Enters config-vlan mode for configuring normal-range and extended-range VLANs.

vlan access-map

Use the **vlan access-map** global configuration command to create or modify a VLAN map entry for VLAN packet filtering. This entry changes the mode to the VLAN access map configuration. Use the **no** form of this command to delete a VLAN map entry. Use the **vlan filter** interface configuration command to apply a VLAN map to one or more VLANs.

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

no vlan access-map *name* [*number*]

Syntax Description	<i>name</i>	Name of the VLAN map.
	<i>number</i>	(Optional) The sequence number of the map entry that you want to create or modify (0 to 65535). If you are creating a VLAN map and the sequence number is not specified, it is automatically assigned in increments of 10, starting from 10. This number is the sequence to insert to, or delete from, a VLAN access-map entry.

Defaults There are no VLAN map entries and no VLAN maps applied to a VLAN.

Command Modes Global configuration

Command History	Release	Modification
	12.1(4)EA1	This command was introduced.

Usage Guidelines In global configuration mode, use this command to create or modify a VLAN map. This entry changes the mode to VLAN access-map configuration, where you can use the **match** access-map configuration command to specify the access lists for IP or non-IP traffic to match and use the **action** command to set whether a match causes the packet to be forwarded or dropped.

In VLAN access map configuration mode, these commands are available:

- **action**: sets the action to be taken (forward or drop).
- **default**: sets a command to its defaults
- **exit**: exits from VLAN access-map configuration mode
- **match**: sets the values to match (IP address or MAC address).
- **no**: negates a command or set its defaults

When you do not specify an entry number (sequence number), it is added to the end of the map.

There can be only one VLAN map per VLAN and it is applied as packets are received by a VLAN.

You can use the **no vlan access-map** *name* [*number*] command with a sequence number to delete a single entry.

In global configuration mode, use the **vlan filter** interface configuration command to apply the map to one or more VLANs.

**Note**

For more information about VLAN map entries, see the software configuration guide for this release.

Examples

This example shows how to create a VLAN map named *vac1* and apply matching conditions and actions to it. If no other entries already exist in the map, this will be entry 10.

```
Switch(config)# vlan access-map vac1
Switch(config-access-map) # match ip address acl1
Switch(config-access-map) # action forward
```

This example shows how to delete VLAN map *vac1*:

```
Switch(config)# no vlan access-map vac1
```

Related Commands

Command	Description
action	Sets the action for the VLAN access map entry.
match (access-map configuration)	Sets the VLAN map to match packets against one or more access lists.
show vlan access-map	Displays information about a particular VLAN access map or all VLAN access maps.
vlan filter	Applies the VLAN access map to one or more VLANs.

vlan database

Use the **vlan database** privileged EXEC command to enter VLAN configuration mode. From this mode, you can add, delete, and modify VLAN configurations for normal-range VLANs and globally propagate these changes by using the VLAN Trunking Protocol (VTP). Configuration information is saved in the VLAN database.

vlan database



Note

VLAN configuration mode is only valid for VLAN IDs 1 to 1005.

Syntax Description

This command has no arguments or keywords.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

You can use the VLAN database configuration commands to configure VLANs 1 to 1005. To configure extended-range VLANs (VLAN IDs 1006 to 4094), use the **vlan (global configuration)** command to enter config-vlan mode. You can also configure VLAN IDs 1 to 1005 by using the **vlan** global configuration command.

To return to the privileged EXEC mode from the VLAN configuration mode, enter the **exit** command.



Note

This command mode is different from other modes because it is session-oriented. When you add, delete, or modify VLAN parameters, the changes are not applied until you exit the session by entering the **apply** or **exit** command. When the changes are applied, the VTP configuration version is incremented. You can also *not* apply the changes to the VTP database by entering **abort**.

When you are in VLAN configuration mode, you can access the VLAN database and make changes by using these commands:

- **vlan**: accesses subcommands to add, delete, or modify values associated with a single VLAN. For more information, see the **vlan (VLAN configuration)** command.
- **vtp**: accesses subcommands to perform VTP administrative functions. For more information, see the **vtp (VLAN configuration)** command.

When you have modified VLAN or VTP parameters, you can use these editing buffer manipulation commands:

- **abort**: exits the mode without applying the changes. The VLAN configuration that was running before you entered VLAN configuration mode continues to be used.
- **apply**: applies current changes to the VLAN database, increments the database configuration revision number, propagates it throughout the administrative domain, and remains in VLAN configuration mode.



Note You cannot use this command when the switch is in VTP client mode.

- **exit**: applies all configuration changes to the VLAN database, increments the database configuration number, propagates it throughout the administrative domain, and returns to privileged EXEC mode.
- **no**: negates a command or set its defaults; valid values are **vlan** and **vtp**.
- **reset**: abandons proposed changes to the VLAN database, resets the proposed database to the implemented VLAN database on the switch, and remains in VLAN configuration mode.
- **show**: displays VLAN database information.
- **show changes** [*vlan-id*]: displays the differences between the VLAN database on the switch and the proposed VLAN database for all normal-range VLAN IDs (1 to 1005) or the specified VLAN ID (1 to 1005).
- **show current** [*vlan-id*]: displays the VLAN database on the switch or on a selected VLAN (1 to 1005).
- **show proposed** [*vlan-id*]: displays the proposed VLAN database or a selected VLAN (1 to 1005) from the proposed database. The proposed VLAN database is not the running configuration until you use the **exit** or **apply** VLAN configuration command.

You can verify that VLAN database changes have been made or aborted by using the **show vlan** privileged EXEC command. This output is different from the **show** VLAN database configuration command output.

Examples

This example shows how to enter the VLAN configuration mode from the privileged EXEC mode and to display VLAN database information:

```
Switch# vlan database
Switch(vlan)# show
VLAN ISL Id: 1
  Name: default
  Media Type: Ethernet
VLAN 802.10 Id: 100001
  State: Operational
  MTU: 1500
  Translational Bridged VLAN: 1002
  Translational Bridged VLAN: 1003

VLAN ISL Id: 2
  Name: VLAN0002
  Media Type: Ethernet
VLAN 802.10 Id: 100002
  State: Operational
  MTU: 1500
```

```
VLAN ISL Id: 1002
  Name: fddi-default
  Media Type: FDDI
  VLAN 802.10 Id: 101002
  State: Operational
  MTU: 1500
  Bridge Type: SRB
  Ring Number: 0
  Translational Bridged VLAN: 1
  Translational Bridged VLAN: 1003
```

<output truncated>

This is an example of output from the **show changes** command:

```
Switch(vlan)# show changes
```

```
DELETED:
  VLAN ISL Id: 4
  Name: VLAN0004
  Media Type: Ethernet
  VLAN 802.10 Id: 100004
  State: Operational
  MTU: 1500
```

```
DELETED:
  VLAN ISL Id: 6
  Name: VLAN0006
  Media Type: Ethernet
  VLAN 802.10 Id: 100006
  State: Operational
  MTU: 1500
```

```
MODIFIED:
  VLAN ISL Id: 7
  Current State: Operational
  Modified State: Suspended
```

This example shows how to display the differences between VLAN 7 in the current database and the proposed database:

```
Switch(vlan)# show changes 7
```

```
MODIFIED:
  VLAN ISL Id: 7
  Current State: Operational
  Modified State: Suspended
```

This is an example of output from the **show current 20** command. It displays only VLAN 20 of the current database.

```
Switch(vlan)# show current 20
VLAN ISL Id: 20
  Name: VLAN0020
  Media Type: Ethernet
  VLAN 802.10 Id: 100020
  State: Operational
  MTU: 1500
```

Related Commands	Command	Description
	show vlan	Displays the parameters for all configured VLANs in the administrative domain.
	shutdown vlan	Shuts down (suspends) local traffic on the specified VLAN.
	vlan (global configuration)	Enters config-vlan mode for configuring normal-range and extended-range VLANs.

vlan dot1q tag native

Use the **vlan dot1q tag native** global configuration command to enable tagging of native VLAN frames on all IEEE 802.1Q trunk ports. Use the **no** form of this command to return to the default setting.

vlan dot1q tag native

no vlan dot1q tag native

Syntax Description

This command has no arguments or keywords.

Defaults

The IEEE 802.1Q native VLAN tagging is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

When enabled, native VLAN packets going out all IEEE 802.1Q trunk ports are tagged.

When disabled, native VLAN packets going out all IEEE 802.1Q trunk ports are not tagged.

You can use this command with the IEEE 802.1Q tunneling feature. This feature operates on an edge switch of a service-provider network and expands VLAN space by using a VLAN-in-VLAN hierarchy and tagging the tagged packets. You must use IEEE 802.1Q trunk ports for sending packets to the service-provider network. However, packets going through the core of the service-provider network might also be carried on IEEE 802.1Q trunks. If the native VLANs of an IEEE 802.1Q trunk match the native VLAN of a tunneling port on the same switch, traffic on the native VLAN is not tagged on the sending trunk port. This command ensures that native VLAN packets on all IEEE 802.1Q trunk ports are tagged.



Note

For more information about IEEE 802.1Q tunneling, see the software configuration guide for this release.

Examples

This example shows how to enable IEEE 802.1Q tagging on native VLAN frames:

```
Switch# configure terminal
Switch (config)# vlan dot1q tag native
Switch (config)# end
```

You can verify your settings by entering the **show vlan dot1q tag native** privileged EXEC command.

■ `vlan dot1q tag native`

Related Commands	Command	Description
	<code>show vlan dot1q tag native</code>	Displays IEEE 802.1Q native VLAN tagging status.

vlan filter

Use the **vlan filter** global configuration command to apply a VLAN map to one or more VLANs. Use the **no** form of this command to remove the map.

vlan filter *mapname* **vlan-list** *list*

no vlan filter *mapname* **vlan-list** *list*

Syntax Description

<i>mapname</i>	Name of the VLAN map entry.
<i>list</i>	The list of one or more VLANs in the form <i>tt, uu-vv, xx, yy-zz</i> , where spaces around commas and dashes are optional. The VLAN ID range is 1 to 4094.

Defaults

There are no VLAN filters.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

To avoid accidentally dropping too many packets and disabling connectivity in the middle of the configuration process, we recommend that you completely define the VLAN access map before applying it to a VLAN. If you apply a nonexistent VLAN map to a VLAN, a warning message appears.



Note

For more information about VLAN map entries, see the software configuration guide for this release.

Examples

This example applies VLAN map entry *map1* to VLANs 20 and 30:

```
Switch(config)# vlan filter map1 vlan-list 20, 30
```

This example shows how to delete VLAN map entry *map1* from VLAN 20:

```
Switch(config)# no vlan filter map1 vlan-list 20
```

You can verify your settings by entering the **show vlan filter** privileged EXEC command.

Related Commands	Command	Description
	show vlan access-map	Displays information about a particular VLAN access map or all VLAN access maps.
	show vlan filter	Displays information about all VLAN filters or about a particular VLAN or VLAN access map.
	vlan access-map	Creates a VLAN map entry for VLAN packet filtering.

vmps reconfirm (privileged EXEC)

Use the **vmps reconfirm** privileged EXEC command to immediately send VLAN Query Protocol (VQP) queries to reconfirm all dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS).

vmps reconfirm

Syntax Description This command has no arguments or keywords.

Defaults No default is defined.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(4)EA1	This command was introduced.

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

```
Switch# vmps reconfirm
```

You can verify your setting by entering the **show vmps** privileged EXEC command and examining the VMPS Action row of the Reconfirmation Status section. The **show vmps** command shows the result of the last time the assignments were reconfirmed either because the reconfirmation timer expired or because the **vmps reconfirm** command was entered.

Related Commands	Command	Description
	show vmps	Displays VQP and VMPS information.
	vmps reconfirm (global configuration)	Changes the reconfirmation interval for the VLAN Query Protocol (VQP) client.

vmps reconfirm (global configuration)

Use the **vmps reconfirm** global configuration command to change the reconfirmation interval for the VLAN Query Protocol (VQP) client. Use the **no** form of this command to return to the default setting.

vmps reconfirm *interval*

no vmps reconfirm

Syntax Description	<i>interval</i>	Reconfirmation interval for VQP client queries to the VLAN Membership Policy Server (VMPS) to reconfirm dynamic VLAN assignments. The range is 1 to 120 minutes.
Defaults	The default reconfirmation interval is 60 minutes.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.1(4)EA1	This command was introduced.
Examples	<p>This example shows how to set the VQP client to reconfirm dynamic VLAN entries every 20 minutes:</p> <pre>Switch(config)# vmps reconfirm 20</pre> <p>You can verify your setting by entering the show vmps privileged EXEC command and examining information in the Reconfirm Interval row.</p>	
Related Commands	Command	Description
	show vmps	Displays VQP and VMPS information.
	vmps reconfirm (privileged EXEC)	Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS.

vmps retry

Use the **vmps retry** global configuration command to configure the per-server retry count for the VLAN Query Protocol (VQP) client. Use the **no** form of this command to return to the default setting.

vmps retry *count*

no vmps retry

Syntax Description	<i>count</i>	Number of attempts to contact the VLAN Membership Policy Server (VMPS) by the client before querying the next server in the list. The range is 1 to 10.
--------------------	--------------	---

Defaults	The default retry count is 3.
----------	-------------------------------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.1(4)EA1	This command was introduced.

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

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

You can verify your setting by entering the **show vmps** privileged EXEC command and examining information in the Server Retry Count row.

Related Commands	Command	Description
	show vmps	Displays VQP and VMPS information.

vmps server

Use the **vmps server** global configuration command to configure the primary VLAN Membership Policy Server (VMPS) and up to three secondary servers. Use the **no** form of this command to remove a VMPS server.

vmps server *ipaddress* [**primary**]

no vmps server [*ipaddress*]

Syntax Description	<i>ipaddress</i>	IP address or host name of the primary or secondary VMPS servers. If you specify a host name, the Domain Name System (DNS) server must be configured.
	primary	(Optional) Determines whether primary or secondary VMPS servers are being configured.

Defaults No primary or secondary VMPS servers are defined.

Command Modes Global configuration

Command History	Release	Modification
	12.1(4)EA1	This command was introduced.

Usage Guidelines

The first server entered is automatically selected as the primary server whether or not **primary** is entered. The first server address can be overridden by using **primary** in a subsequent command.

If a member switch in a cluster configuration does not have an IP address, the cluster does not use the VMPS server configured for that member switch. Instead, the cluster uses the VMPS server on the command switch, and the command switch proxies the VMPS requests. The VMPS server treats the cluster as a single switch and uses the IP address of the command switch to respond to requests.

When using the **no** form without specifying the *ipaddress*, all configured servers are deleted. If you delete all servers when dynamic-access ports are present, the switch cannot forward packets from new sources on these ports because it cannot query the VMPS.

Examples This example shows how to configure the server with IP address 191.10.49.20 as the primary VMPS server. The servers with IP addresses 191.10.49.21 and 191.10.49.22 are configured as secondary servers:

```
Switch(config)# vmps server 191.10.49.20 primary
Switch(config)# vmps server 191.10.49.21
Switch(config)# vmps server 191.10.49.22
```

This example shows how to delete the server with IP address 191.10.49.21:

```
Switch(config)# no vmips server 191.10.49.21
```

You can verify your setting by entering the **show vmips** privileged EXEC command and examining information in the VMPS Domain Server row.

Related Commands

Command	Description
show vmips	Displays VQP and VMPS information.

vtp (global configuration)

Use the **vtp** global configuration command to set or modify the VLAN Trunking Protocol (VTP) configuration characteristics. Use the **no** form of this command to remove the settings or to return to the default settings.

```
vtp { domain domain-name | file filename | interface name | mode { client | server | transparent }
      | password password | pruning | version number }
```

```
no vtp { file | interface | mode | password | pruning | version }
```

Syntax Description

domain <i>domain-name</i>	Specify the VTP domain name, an ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the switch. The domain name is case sensitive.
file <i>filename</i>	Specify the Cisco IOS file system file where the VTP VLAN configuration is stored.
interface <i>name</i>	Specify the name of the interface providing the VTP ID updated for this device.
mode	Specify the VTP device mode as client, server, or transparent.
client	Place the switch in VTP client mode. A switch in VTP client mode is enabled for VTP, and can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on the switch. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.
server	Place the switch in VTP server mode. A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on the switch. The switch can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.
transparent	Place the switch in VTP transparent mode. A switch in VTP transparent mode is disabled for VTP, does not send 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. When VTP mode is transparent, the mode and domain name are saved in the switch running configuration file, and you can save them in the switch startup configuration file by entering the copy running-config startup config privileged EXEC command.
password <i>password</i>	Set the administrative domain password for the generation of the 16-byte secret value used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements. The password can be an ASCII string from 1 to 32 characters. The password is case sensitive.
pruning	Enable VTP pruning on the switch.
version <i>number</i>	Set VTP version to version 1 or version 2.

Defaults

The default filename is *flash:vlan.dat*.

The default mode is server mode.

No domain name or password is defined.

No password is configured.

Pruning is disabled.

The default version is version 1.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(9)EA1	The domain and mode keywords were added. The if-id keyword was replaced by the interface keyword.
12.1(11)EA1	The password , pruning , and version keywords were added.

Usage Guidelines

When you save VTP mode and domain name and VLAN configurations in the switch startup configuration file and reboot the switch, the VTP and VLAN configurations are determined by these conditions:

- If both the VLAN database and the configuration file show the VTP mode as transparent and the VTP domain names match, the VLAN database is ignored. The VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the startup VTP mode is server mode, or the startup VTP mode or domain names do not match the VLAN database, VTP mode and VLAN configuration for the first 1005 VLANs are determined by VLAN database information, and VLANs greater than 1005 are configured from the switch configuration file.
- If the image on the switch or the configuration file is earlier than Cisco IOS Release 12.1(9)EA1, the switch reboots using the information in the VLAN database.

The **vtp file filename** cannot be used to load a new database; it renames only the file in which the existing database is stored.

Follow these guidelines when configuring a VTP domain name:

- The switch is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the switch does not send any VTP advertisements even if changes occur to the local VLAN configuration. The switch leaves the no-management-domain state after it receives the first VTP summary packet on any port that is trunking or after you configure a domain name by using the **vtp domain** command. If the switch receives its domain from a summary packet, it resets its configuration revision number to 0. After the switch leaves the no-management-domain state, it can no be configured to re-enter it until you clear the NVRAM and reload the software.
- Domain names are case-sensitive.
- After you configure a domain name, it cannot be removed. You can only reassign it to a different domain.

Follow these guidelines when setting VTP mode:

- The **no vtp mode** command returns the switch to VTP server mode.
- The **vtp mode server** command is the same as **no vtp mode** except that it does not return an error if the switch is not in client or transparent mode.
- If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. If you have switches in client mode, be sure to make all VTP or VLAN configuration changes on a switch in server mode. If the receiving switch is in server mode or transparent mode, the switch configuration is not changed.
- Switches in transparent mode do not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to other switches in the network.
- If you change the VTP or VLAN configuration on a switch that is in server mode, that change is propagated to all the switches in the same VTP domain.
- The **vtp mode transparent** command disables VTP from the domain but does not remove the domain from the switch.
- The VTP mode must be transparent for you to add extended-range VLANs or for VTP and VLAN information to be saved in the running configuration file.
- If extended-range VLANs are configured on the switch and you attempt to set the VTP mode to server or client, you receive an error message, and the configuration is not allowed.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.

Follow these guidelines when setting a VTP password:

- Passwords are case sensitive. Passwords should match on all switches in the same domain.
- When you use the **no vtp password** form of the command, the switch returns to the no-password state.

Follow these guidelines when setting VTP pruning:

- VTP pruning removes information about each pruning-eligible VLAN from VTP updates if there are no stations belonging to that VLAN.
- If you enable pruning on the VTP server, it is enabled for the entire management domain for VLAN IDs 1 to 1005.
- Only VLANs in the pruning-eligible list can be pruned.
- Pruning is supported with VTP version 1 and version 2.

Follow these guidelines when setting the VTP version:

- Toggling the version 2 (v2) mode state modifies parameters of certain default VLANs.
- Each VTP switch automatically detects the capabilities of all the other VTP devices. To use version 2, all VTP switches in the network must support version 2; otherwise, you must configure them to operate in VTP version 1 mode.
- If all switches in a domain are VTP version 2-capable, you need only to configure version 2 on one switch; the version number is then propagated to the other version-2 capable switches in the VTP domain.

- If you are using VTP in a Token Ring environment, VTP version 2 must be enabled.
- If you are configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, you must use version 2.
- If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use version 1.

You cannot save password, pruning, and version configurations in the switch configuration file.

Examples

This example shows how to rename the filename for VTP configuration storage to *vtpfilename*:

```
Switch(config)# vtp file vtpfilename
```

This example shows how to clear the device storage filename:

```
Switch(config)# no vtp file vtpconfig
Clearing device storage filename.
```

This example shows how to specify the name of the interface providing the VTP updater ID for this device:

```
Switch(config)# vtp interface fastethernet
```

This example shows how to set the administrative domain for the switch:

```
Switch(config)# vtp domain OurDomainName
```

This example shows how to place the switch in VTP transparent mode:

```
Switch(config)# vtp mode transparent
```

This example shows how to configure the VTP domain password:

```
Switch(config)# vtp password ThisIsOurDomain'sPassword
```

This example shows how to enable pruning in the VLAN database:

```
Switch(config)# vtp pruning
Pruning switched ON
```

This example shows how to enable version 2 mode in the VLAN database:

```
Switch(config)# vtp version 2
```

You can verify your settings by entering the **show vtp status** privileged EXEC command.

Related Commands

Command	Description
show vtp status	Displays the VTP statistics for the switch and general information about the VTP management domain status.
vtp (VLAN configuration)	Configures VTP domain-name, password, pruning, version, and mode.

vtp (privileged EXEC)

Use the **vtp** privileged EXEC command to configure the VLAN Trunking Protocol (VTP) password, pruning, and version. Use the **no** form of this command to return to the default settings.

```
vtp {password password | pruning | version number}
```

```
no vtp {password | pruning | version}
```



Note

Beginning with release 12.1(11)EA1, these keywords are available in the **vtp** global configuration command. This command will become obsolete in a future release.

Syntax Description

password <i>password</i>	Set the administrative domain password for the generation of the 16-byte secret value used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements. The password can be an ASCII string from 1 to 32 characters. The password is case sensitive.
pruning	Enable VTP pruning on the switch.
version <i>number</i>	Set VTP version to version 1 or version 2.

Defaults

No password is configured.
Pruning is disabled.
The default version is version 1.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

Passwords are case sensitive. Passwords should match on all switches in the same domain.

When you use the **no vtp password** form of the command, the switch returns to the no-password state. VTP pruning removes information about each pruning-eligible VLAN from VTP updates if there are no stations belonging to that VLAN.

If you enable pruning on the VTP server, it is enabled for the entire management domain for VLAN IDs 1 to 1005.

Only VLANs in the pruning-eligible list can be pruned.

Pruning is supported with VTP version 1 and version 2.

toggling the version 2 (v2) mode state modifies parameters of certain default VLANs.

Each VTP switch automatically detects the capabilities of all the other VTP devices. To use version 2, all VTP switches in the network must support version 2; otherwise, you must configure them to operate in VTP version 1 mode.

If all switches in a domain are VTP version 2-capable, you need only to configure version 2 on one switch; the version number is then propagated to the other version-2 capable switches in the VTP domain.

If you are using VTP in a Token Ring environment, VTP version 2 must be enabled.

If you are configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, you must use version 2.

If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use version 1.

You cannot save password, pruning, and version configuration in the switch configuration file.

Examples

This example shows how to configure the VTP domain password:

```
Switch# vtp password ThisIsOurDomain'sPassword
```

This example shows how to enable pruning in the VLAN database:

```
Switch# vtp pruning
Pruning switched ON
```

This example shows how to enable version 2 mode in the VLAN database:

```
Switch# vtp version 2
```

You can verify your setting by entering the **show vtp status** privileged EXEC command.

Related Commands

Command	Description
show vtp status	Displays the VTP statistics for the switch and general information about the VTP management domain status.
switchport trunk pruning	Configures the VLAN pruning-eligible list for ports in trunking mode.
vtp (global configuration)	Configures the VTP filename, interface, domain-name, and mode, which can be saved in the switch configuration file.
vtp (VLAN configuration)	Configures all VTP characteristics but cannot be saved to the switch configuration file.

vtp (VLAN configuration)

Use the **vtp** VLAN configuration command to configure VLAN Trunking Protocol (VTP) characteristics. You access VLAN configuration mode by entering the **vlan database** privileged EXEC command. Use the **no** form of this command to return to the default settings, disable the characteristic, or remove the password.

```
vtp {domain domain-name | password password | pruning | v2-mode | {server | client | transparent}}
```

```
no vtp {client | password | pruning | transparent | v2-mode}
```



Note

VTP configuration in VLAN configuration mode is saved in the VLAN database when applied.

Syntax Description

domain <i>domain-name</i>	Set the VTP domain name by entering an ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the switch. The domain name is case sensitive.
password <i>password</i>	Set the administrative domain password for the generation of the 16-byte secret value used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements. The password can be an ASCII string from 1 to 32 characters. The password is case sensitive.
pruning	Enable pruning in the VTP administrative domain. VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN.
v2-mode	Enable VLAN Trunking Protocol (VTP) version 2 in the administrative domains.
client	Place the switch in VTP client mode. 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 send VTP advertisements until it receives advertisements to initialize its VLAN database.
server	Place the switch in VTP server mode. A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.
transparent	Place the switch in VTP transparent mode. A switch in VTP transparent mode is disabled for VTP, does not send 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.

Defaults

The default mode is server mode.
 No domain name is defined.
 No password is configured.
 Pruning is disabled.
 VTP version 2 (v2 mode) is disabled.

Command Modes

VLAN configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

If VTP mode is transparent, the mode and domain name are saved in the switch running configuration file, and you can save the configuration in the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

Follow these guidelines when setting VTP mode:

- The **no vtp client** and **no vtp transparent** forms of the command return the switch to VTP server mode.
- The **vtp server** command is the same as **no vtp client** or **no vtp transparent** except that it does not return an error if the switch is not in client or transparent mode.
- If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. If you have switches in client mode, make sure to make all VTP or VLAN configuration changes on a switch in server mode. If the receiving switch is in server mode or transparent mode, the switch configuration is not changed.
- Switches in transparent mode do not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to other switches in the network.
- If you make a change to the VTP or VLAN configuration on a switch in server mode, that change is propagated to all the switches in the same VTP domain.
- The **vtp transparent** command disables VTP from the domain but does not remove the domain from the switch.
- The VTP mode must be transparent for you to add extended-range VLANs or for the VTP and the VLAN configurations to be saved in the running configuration file.
- If extended-range VLANs are configured on the switch and you attempt to set the VTP mode to server or client, you receive an error message and the configuration is not allowed.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.

Follow these guidelines when configuring a VTP domain name:

- The switch is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the switch does not send any VTP advertisements even if changes occur to the local VLAN configuration. The switch leaves the no-management-domain state after receiving the first VTP summary packet on any port that is currently trunking or after configuring a domain name with the **vtp domain** command. If the switch receives its domain from a summary packet, it resets its configuration revision number to zero. After the switch leaves the no-management-domain state, it can never be configured to reenter it until you clear the NVRAM and reload the software.
- Domain names are case sensitive.
- After you configure a domain name, it cannot be removed. You can reassign it only to a different domain.

Follow these guidelines when configuring a VTP password:

- Passwords are case sensitive. Passwords should match on all switches in the same domain.
- When the **no vtp password** form of the command is used, the switch returns to the no-password state.

Follow these guidelines when enabling VTP pruning:

- If you enable pruning on the VTP server, it is enabled for the entire management domain.
- Only VLANs included in the pruning-eligible list can be pruned.
- Pruning is supported with VTP version 1 and version 2.

Follow these guidelines when enabling VTP version 2 (v2-mode):

- Toggling the version (v2-mode) state modifies certain parameters of certain default VLANs.
- Each VTP switch automatically detects the capabilities of all the other VTP devices. To use VTP version 2, all VTP switches in the network must support version 2; otherwise, you must configure them to operate in VTP version 1 (**no vtp v2-mode**).
- If all switches in a domain are VTP version 2-capable, you need only to enable VTP version 2 on one switch; the version number is then propagated to the other version-2 capable switches in the VTP domain.
- If you are using VTP in a Token Ring environment or configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, VTP version 2 (**v2-mode**) must be enabled.
- If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use VTP version 1.

Examples

This example shows how to place the switch in VTP transparent mode:

```
Switch(vlan)# vtp transparent
Setting device to VTP TRANSPARENT mode.
```

This example shows how to set the administrative domain for the switch:

```
Switch(vlan)# vtp domain OurDomainName
Changing VTP domain name from cisco to OurDomainName
```

This example shows how to configure the VTP domain password:

```
Switch(vlan)# vtp password private
Setting device VLAN database password to private.
```

This example shows how to enable pruning in the proposed new VLAN database:

```
Switch(vlan)# vtp pruning
Pruning switched ON
```

This example shows how to enable v2 mode in the proposed new VLAN database:

```
Switch(vlan)# vtp v2-mode
V2 mode enabled.
```

You can verify your settings by entering the **show vtp status** privileged EXEC command.

Related Commands

Command	Description
show vtp status	Displays the VTP statistics for the switch and general information about the VTP management domain status.
switchport trunk pruning	Configures the VLAN pruning-eligible list for ports in trunking mode.
vtp (global configuration)	Configures the VTP filename, interface, domain-name, and mode.

wrr-queue bandwidth

Use the **wrr-queue bandwidth** interface configuration command to assign weighted round robin (WRR) weights to the egress queues on Gigabit-capable ports and 10/100 Ethernet ports. The ratio of the weights is the ratio of frequency in which the WRR scheduler dequeues packets from each queue. Use the **no** form of this command to return to the default setting.

```
wrr-queue bandwidth weight1 weight2 weight3 weight4
```

```
no wrr-queue bandwidth
```

Syntax Description	<i>weight1 weight2 weight3 weight4</i>	The ratio of <i>weight1</i> , <i>weight2</i> , <i>weight3</i> , and <i>weight4</i> determines the ratio of the frequency in which the WRR scheduler dequeues packets. Separate each value with a space. The range is 1 to 65536.
---------------------------	--	--

Defaults	Weight1, weight2, weight3, and weight4 are 25 (1/4 of the bandwidth is allocated to each queue).
-----------------	--

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.1(4)EA1	This command was introduced.
	12.1(13)EA1	The range changed from 0 to 65536 to 1 to 65536.

Usage Guidelines	<p>The absolute value of each weight is meaningless, and only the ratio of parameters is used.</p> <p>WRR allows bandwidth sharing at the egress port.</p> <p>All four queues participate in the WRR unless the expedite queue (queue 4) is enabled, in which case <i>weight4</i> is ignored (not used in the ratio calculation). The expedite queue is a priority queue, and it is serviced until empty before the other queues are serviced. You enable the expedite queue by using the priority-queue out interface configuration command.</p> <p>A weight of 1 means that the minimum bandwidth is allocated for that queue.</p> <p>To allocate no bandwidth for a queue, use the wrr-queue cos-map interface configuration command. The available bandwidth is shared among the remaining queues.</p>
-------------------------	--

Examples	<p>This example shows how to configure the weight ratio of the WRR scheduler running on the egress queues. In this example, four queues are used (no expedite queue), and the ratio of the bandwidth allocated for each queue is $1/(1+2+3+4)$, $2/(1+2+3+4)$, $3/(1+2+3+4)$, and $4/(1+2+3+4)$, which is 1/10, 1/5, 3/10, and 2/5 for queues 1, 2, 3, and 4.</p>
-----------------	---

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# wrr-queue bandwidth 1 2 3 4
```

This example shows how to configure the weight ratio of WRR if the expedite queue is enabled. Three queues participate in WRR, and the bandwidth allocated for each queue is $1/(1+2+3)$, $2/(1+2+3)$, $3/(1+2+3)$, which is 1/6, 1/3, and 1/2 for queues 1, 2, and 3. The last parameter, 9, is not used to calculate the bandwidth ratio.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# priority-queue out
Switch(config-if)# wrr-queue bandwidth 1 2 3 9
```

You can verify your settings by entering the **show mls qos interface queueing** privileged EXEC command.

Related Commands

Command	Description
show mls qos interface	Displays quality of service (QoS) information.
wrr-queue cos-map	Maps assigned class of service (CoS) values to select one of the egress queues.
wrr-queue queue-limit	Configures the sizes of the egress queues on Gigabit-capable Ethernet ports.

wrr-queue cos-map

Use the **wrr-queue cos-map** interface configuration command to map assigned class of service (CoS) values to select one of the egress queues. Use the form **no** of this command to return the CoS map to the default setting.

```
wrr-queue cos-map queue-id cos1 ... cos8
```

```
no wrr-queue cos-map [queue-id [cos1 ... cos8]]
```

Syntax Description

<i>queue-id</i>	ID of the egress queue. The range is 1 to 4, where 4 can be configured as the expedite queue.
<i>cos1 ... cos8</i>	CoS values that are mapped to select a queue. Enter up to eight CoS values. Separate each value with a space. The range is 0 to 7.

Defaults

Table 2-35 shows the default CoS-to-egress-queue map when QoS is enabled.

Table 2-35 Default CoS-to-Egress-Queue Map when QoS is Enabled

CoS Value	Queue Selected
0, 1	1
2, 3	2
4, 5	3
6, 7	4

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(12c)EA1	CoS values were added to the no form of this command.

Usage Guidelines

When quality of service (QoS) is disabled, all CoS values are mapped to queue 1.

You can use this command to distribute traffic into different queues, where each queue is configured with different weighted round robin (WRR) and Weighted Random Early Detection (WRED) parameters.

You enable the expedite queue by using the **priority-queue out** interface configuration command.

Examples

This example shows how to map CoS values 0 and 1 to queue 1, 2 and 3 to queue 2, 4 and 5 to queue 3, 6 and 7 to queue 4:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# wrr-queue cos-map 1 0 1
Switch(config-if)# wrr-queue cos-map 2 2 3
Switch(config-if)# wrr-queue cos-map 3 4 5
Switch(config-if)# wrr-queue cos-map 4 6 7
```

You can verify your settings by entering the **show mls qos interface queueing** privileged EXEC command.

Related Commands

Command	Description
show mls qos interface queueing	Displays the queueing strategy (WRR, priority queueing), the weights corresponding to the queues, and the CoS-to-egress-queue map.
wrr-queue dscp-map	Maps DSCP values to the tail-drop or WRED thresholds of the egress queues.

wrr-queue dscp-map

Use the **wrr-queue dscp-map** interface configuration command on an ingress Gigabit-capable Ethernet port to map the Differentiated Services Code Point (DSCP) values to the tail-drop or Weighted Random Early Detection (WRED) thresholds of the egress queues. Use the form **no** of this command to return the DSCP map to the default setting.

```
wrr-queue dscp-map threshold-id dscp1 ... dscp8
```

```
no wrr-queue dscp-map [threshold-id]
```

Syntax Description		
	<i>threshold-id</i>	Threshold ID of the queue. The range is 1 to 2.
	<i>dscp1 ... dscp8</i>	DSCP values that are mapped to a threshold ID. Enter up to eight DSCP values per command. Separate each value with a space. The range is 0 to 63.

Defaults All DSCP values are mapped to threshold 1.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(4)EA1	This command was introduced.

Usage Guidelines Up to eight DSCP values can be entered per command.

Examples This example shows how to map DSCP values 0 to 9 to threshold 1 and 10 to 14 to threshold 2:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# wrr-queue dscp-map 1 0 1 2 3 4 5 6 7
Switch(config-if)# wrr-queue dscp-map 1 8 9
Switch(config-if)# wrr-queue dscp-map 2 10 11 12 13 14
```

You can verify your settings by entering the **show running-config** or the **show mls qos interface interface-id** privileged EXEC command.

Related Commands	Command	Description
	show mls qos interface	Displays quality of service (QoS) information.
	wrr-queue cos-map	Maps assigned class of service (CoS) ingress values to select one of the egress queues.
	wrr-queue random-detect max-threshold	Enables WRED and assigns two WRED threshold values to an egress queue of a Gigabit-capable Ethernet port.
	wrr-queue threshold	Assigns tail-drop threshold percentages to an egress queue of a Gigabit-capable Ethernet port.

wrr-queue min-reserve

Use the **wrr-queue min-reserve** interface configuration command to assign a minimum-reserve level to a particular egress queue of a 10/100 Ethernet port. Use the **no** form of this command to return to the default setting.

wrr-queue min-reserve *queue-id min-reserve-level*

no wrr-queue min-reserve *queue-id*

Syntax Description

<i>queue-id</i>	ID of the egress queue. The range is 1 to 4.
<i>min-reserve-level</i>	One of the eight minimum-reserve levels configured with the mls qos min-reserve global configuration command.

Defaults

Queue 1 selects minimum-reserve level 1, queue 2 selects minimum-reserve level 2, queue 3 selects minimum-reserve level 3, and queue 4 selects minimum-reserve level 4.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA1	This command was introduced.

Usage Guidelines

You can assign the same minimum-reserve level to multiple queues. Each queue is allocated the same amount of buffer space.

When you enter this command, the queue is temporarily shut down during the hardware reconfiguration, and the switch drops newly arrived packets to this queue.

Examples

This example shows how to configure minimum-reserve level 5 to 20 packets and assign minimum-reserve level 5 to egress queue 1 on a port:

```
Switch(config)# mls qos min-reserve 5 20
Switch(config)# interface fastethernet0/1
Switch(config-if)# wrr-queue min-reserve 1 5
```

You can verify your settings by entering the **show mls qos interface buffers** privileged EXEC command.

Related Commands

Command	Description
mls qos min-reserve	Configures the minimum-reserve levels on 10/100 Ethernet ports.
show mls qos interface	Displays quality of service (QoS) information.

wrr-queue queue-limit

Use the **wrr-queue queue-limit** interface configuration command to configure the sizes of the egress queues on Gigabit-capable Ethernet ports. Use the **no** form of this command to return to the default setting.

```
wrr-queue queue-limit weight1 weight2 weight3 weight4
```

```
no wrr-queue queue-limit
```

Syntax Description

<i>weight1 weight2 weight3 weight4</i>	Ratio of <i>weight1</i> , <i>weight2</i> , <i>weight3</i> , and <i>weight4</i> determines the ratio of the sizes of the queues. Separate each value with a space. The weight range is 1 to 100.
--	---

Defaults

Weight1, weight2, weight3, and weight4 are 25 (1/4 of the buffer size is allocated to each queue).

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The relative size differences in the numbers show the relative differences in the queue sizes.

On Gigabit-capable Ethernet ports, the total size of the queue can vary depending on the amount of RAM in the switch.

When you enter this command, the queue is temporarily shut down during the hardware reconfiguration, and the switch drops newly arrived packets to this queue.

Examples

This example shows how to configure the buffer size ratio of the four queues. The ratio of the buffer allocated for each queue is 1/10, 1/5, 3/10 and 2/5 to queue 1, 2, 3, and 4. (Queue 4 is four times larger than queue 1, twice as large as queue 2, and 1.33 times as large as queue 3.)

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# wrr-queue queue-limit 1 2 3 4
```

You can verify your settings by entering the **show mls qos interface buffers** privileged EXEC command.

Related Commands	Command	Description
	show mls qos interface	Displays QoS information.
	wrr-queue bandwidth	Assigns weighted round robin (WRR) weights to the egress queues.
	wrr-queue min-reserve	Configures the sizes of the minimum-reserve threshold values of the queues on 10/100 Ethernet ports.

wrr-queue random-detect max-threshold

Use the **wrr-queue random-detect max-threshold** interface configuration command to enable Weighted Random Early Detection (WRED) and assign two WRED threshold values to an egress queue of a Gigabit-capable Ethernet port. Use the **no** form of this command to return to the default setting.

wrr-queue random-detect max-threshold *queue-id* *threshold-percentage1* *threshold-percentage2*

no wrr-queue random-detect max-threshold *queue-id*

Syntax Description

<i>queue-id</i>	ID of the queue. The range is 1 to 4, where 4 can be configured as the expedite queue.
<i>threshold-percentage1</i> <i>threshold-percentage2</i>	Maximum threshold percentage values configured per queue. Each threshold percentage represents (average queue size divided by queue size) where WRED starts dropping packets. The WRED minimum threshold value is always 0 when the average queue size equals the allocated queue size. Separate each value with a space. The percentage range is 1 to 100.

Defaults

WRED is disabled, and no thresholds are configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

Quality of service (QoS) uses the DSCP-to-threshold map to determine which Differentiated Services Code Points (DSCPs) are mapped to threshold 1 and threshold 2. After a threshold is exceeded, WRED randomly begins to drop packets assigned to this threshold. As the queue limit is approached, WRED continues to drop more and more packets. When the queue limit is reached, WRED drops all packets assigned to the threshold.

You can enable WRED on the egress expedite queue by using the **priority-queue out** interface configuration command.

You configure the DSCP-to-threshold map by using the **wrr-queue dscp-map** interface configuration command on the ingress interface.

The **wrr-queue random-detect max-threshold** and the **wrr-queue threshold** commands are mutually exclusive, and only WRED or tail-drop thresholds can be configured.

When you enter the **no wrr-queue random-detect max-threshold** *queue-id* command, tail drop is enabled with the maximum threshold values set to 100 percent.

Examples

This example shows how to configure the WRED maximum threshold values for queue 1 from 50 to 100 percent, for queue 2 from 70 to 100 percent, for queue 3 from 50 to 100 percent, and for queue 4 from 70 to 100 percent:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# wrr-queue random-detect max-threshold 1 50 100
Switch(config-if)# wrr-queue random-detect max-threshold 2 70 100
Switch(config-if)# wrr-queue random-detect max-threshold 3 50 100
Switch(config-if)# wrr-queue random-detect max-threshold 4 70 100
```

You can verify your settings by entering the **show mls qos interface buffers** privileged EXEC command.

Related Commands

Command	Description
show mls qos interface	Displays QoS information.
wrr-queue dscp-map	Maps DSCP values to the tail-drop or WRED thresholds of the egress queues.
wrr-queue queue-limit	Configures the sizes of the egress queues on Gigabit-capable Ethernet ports.

wrr-queue threshold

Use the **wrr-queue threshold** interface configuration command to assign tail-drop threshold percentages to each egress queue of a Gigabit-capable Ethernet port. Use the **no** form of this command to return to the default setting.

```
wrr-queue threshold queue-id threshold-percentage1 threshold-percentage2
```

```
no wrr-queue threshold queue-id
```

Syntax Description

<i>queue-id</i>	ID of the egress queue. The range is 1 to 4, where the higher ID has a higher priority.
<i>threshold-percentage1</i> <i>threshold-percentage2</i>	Two tail-drop threshold percentage values. Each threshold value is a percentage of the total number of queue descriptors allocated for the queue. Separate each value with a space. The percentage range is 1 to 100.

Defaults

When QoS is enabled, tail-drop is enabled.

The tail-drop thresholds are 100 percent for both thresholds 1 and 2.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

QoS uses the DSCP-to-threshold map to determine which Differentiated Services Code Points (DSCPs) are mapped to threshold 1 and threshold 2. If threshold 1 is exceeded, packets with DSCPs assigned to this threshold are dropped until the threshold is no longer exceeded. However, packets assigned to threshold 2 continue to be queued and sent as long as the second threshold is not exceeded.

You configure the DSCP-to-threshold map by using the **wrr-queue dscp-map** interface configuration command on the ingress interface.

The **wrr-queue threshold** and the **wrr-queue random-detect threshold** commands are mutually exclusive, and only tail-drop or Weighted Random Early Detection (WRED) thresholds can be configured.

Examples

This example shows how to configure the tail-drop thresholds of the four queues. The queue 1 thresholds are 50% and 100%; the queue 2 thresholds are 70% and 100%; queue 3 thresholds are 80% and 100%; queue 4 thresholds are 100% and 100%.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# wrr-queue threshold 1 50 100
Switch(config-if)# wrr-queue threshold 2 70 100
Switch(config-if)# wrr-queue threshold 3 80 100
Switch(config-if)# wrr-queue threshold 4 100 100
```

You can verify your settings by entering the **show mls qos interface buffers** privileged EXEC command.

Related Commands

Command	Description
show mls qos interface	Displays QoS information.
wrr-queue dscp-map	Maps DSCP values to the tail-drop or WRED thresholds of the egress queues.
wrr-queue queue-limit	Configures the sizes of the egress queues on Gigabit-capable Ethernet ports.