

tunnel flow egress-records

To create a NetFlow record for packets that are encapsulated by a generic routing encapsulation (GRE) tunnel when both NetFlow and Cisco Express Forwarding (CEF) are enabled, use the **tunnel flow egress-records** command in interface configuration mode. To disable NetFlow record creation, use the **no** form of this command.

tunnel flow egress-records

no tunnel flow egress-records

Syntax Description This command has no arguments or keywords.

Defaults A NetFlow record for encapsulated packets is not created.

Command Modes Interface configuration

Command History	Release	Modification
	12.2(2)T	This command was introduced.

Usage Guidelines When this command is enabled on a GRE tunnel with both CEF and NetFlow enabled, a NetFlow record is created for packets that are encapsulated by the tunnel.

Examples The following example shows how to enable NetFlow record creation:

```
Router(config-if)# tunnel flow egress-records
```

Related Commands	Command	Description
	show ip cache flow	Displays NetFlow switching statistics.

tunnel mode mpls traffic-eng

To set the mode of a tunnel to Multiprotocol Label Switching (MPLS) for traffic engineering, use the **tunnel mode mpls traffic-eng** command in interface configuration mode. To disable this feature, use the **no** form of this command.

tunnel mode mpls traffic-eng

no tunnel mode mpls traffic-eng

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Interface configuration

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines This command specifies that the tunnel interface is for an MPLS traffic engineering tunnel and enables the various tunnel MPLS configuration options.

Examples The following example shows how to set the mode of the tunnel to MPLS traffic engineering:

```
Router(config-if)# tunnel mode mpls traffic-eng
```

Related Commands	Command	Description
	tunnel mpls traffic-eng affinity	Configures an affinity for an MPLS traffic engineering tunnel.
	tunnel mpls traffic-eng autoroute announce	Instructs the Interior Gateway Protocol (IGP) to use the tunnel in its enhanced shortest path first algorithm (SPF) calculation (if the tunnel is up).
	tunnel mpls traffic-eng bandwidth	Configures the bandwidth required for an MPLS traffic engineering tunnel.
	tunnel mpls traffic-eng path-option	Configures a path option.
	tunnel mpls traffic-eng priority	Configures setup and reservation priority for an MPLS traffic engineering tunnel.

tunnel mpls traffic-eng affinity

To configure an affinity (the properties the tunnel requires in its links) for a Multiprotocol Label Switching (MPLS) traffic engineering tunnel, use the **tunnel mpls traffic-eng affinity** command in interface configuration mode. To disable the MPLS traffic engineering tunnel affinity, use the **no** form of this command.

tunnel mpls traffic-eng affinity *properties* [**mask** *mask value*]

no tunnel mpls traffic-eng affinity *properties* [**mask** *mask value*]

Syntax Description

<i>properties</i>	Attribute values required for links carrying this tunnel. A 32-bit decimal number. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.
mask <i>mask value</i>	(Optional) Link attribute to be checked. A 32-bit decimal number. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.

Defaults

properties: 0X00000000
mask value: 0X0000FFFF

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines

The affinity determines the attributes of the links that this tunnel will use (that is, the attributes for which the tunnel has an affinity). The attribute mask determines which link attribute the router should check. If a bit in the mask is 0, an attribute value of a link or that bit is irrelevant. If a bit in the mask is 1, the attribute value of a link and the required affinity of the tunnel for that bit must match.

A tunnel can use a link if the tunnel affinity equals the link attributes and the tunnel affinity mask.

Any properties set to 1 in the affinity should also be 1 in the mask. In other words, affinity and mask should be set as follows:

```
tunnel_affinity = (tunnel_affinity and tunnel_affinity_mask)
```

Examples

The following example shows how to set the affinity of the tunnel to 0x0101 mask 0x303:

```
Router(config-if)# tunnel mpls traffic-eng affinity 0x0101 mask 0x303
```

Related Commands

Command	Description
mpls traffic-eng attribute-flags	Sets the attributes for the interface.
tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for traffic engineering.

tunnel mpls traffic-eng auto-bw

To configure a tunnel for automatic bandwidth adjustment and to control the manner in which the bandwidth for a tunnel is adjusted, use the **tunnel mpls traffic-eng auto-bw** command in interface configuration mode. To disable automatic bandwidth adjustment for a tunnel, use the **no** form of this command.

```
tunnel mpls traffic-eng auto-bw [collect-bw] [frequency seconds] [max-bw number]
[min-bw number]
```

```
no tunnel mpls traffic-eng auto-bw
```

Syntax Description

collect-bw	(Optional) Collects output rate information for the tunnel, but does not adjust the tunnel's bandwidth.
frequency <i>seconds</i>	(Optional) The interval between bandwidth adjustments. The specified interval can be from 300 to 604800 seconds. Do not specify a value lower than the output rate sampling interval specified in the mpls traffic-eng auto-bw global configuration command.
max-bw <i>number</i>	(Optional) Maximum automatic bandwidth, in kbps, for this tunnel. The value can be from 0 to 4294967295.
min-bw <i>number</i>	(Optional) Minimum automatic bandwidth, in kbps, for this tunnel. The value can be from 0 to 4294967295.

Defaults

If the command is entered with no optional keywords or arguments, automatic bandwidth adjustment for the tunnel is enabled, with adjustments made every 24 hours and with no constraints on the bandwidth adjustments made.

If the **collect-bw** keyword is entered, the tunnel's bandwidth is sampled but not adjusted, and the other keywords, if any, are ignored.

If the **collect-bw** keyword is not entered and some, but not all of the other keywords are entered, the defaults for the options not entered are: **frequency**, every 24 hours; **min-bw**, unconstrained (0); **max-bw**, unconstrained.

Command Modes

Interface configuration

Command History

Release	Modification
Release 12.2(4)T	This command was introduced.

Usage Guidelines

To sample the bandwidth used by a tunnel without automatically adjusting it, specify the **collect-bw** keyword in the **tunnel mpls traffic-eng auto-bw** command.

If you enter the **tunnel mpls traffic-eng auto-bw** command without the **collect-bw** keyword, the tunnel's bandwidth is adjusted to the largest average output rate sampled for the tunnel since the last bandwidth adjustment for the tunnel was made.

To constrain the bandwidth adjustment that can be made to a tunnel, use the **max-bw** and/or **min-bw** keywords and specify the permitted maximum allowable bandwidth and/or minimum allowable bandwidth, respectively.

The **no** form of the **tunnel mpls traffic-eng auto-bw** command disables bandwidth adjustment for the tunnel and restores the configured bandwidth for the tunnel bandwidth where “configured bandwidth” is determined as follows:

- If the tunnel bandwidth was explicitly configured via the **tunnel mpls traffic-eng bandwidth** command after the running configuration was written (if at all) to the startup configuration, the “configured bandwidth” is the bandwidth specified by that command.
- Otherwise, the “configured bandwidth” is the bandwidth specified for the tunnel in the startup configuration.

**Note**

When you save the router configuration, the current bandwidth (not the originally configured bandwidth) is saved for tunnels with automatic bandwidth enabled.

**Note**

Each **tunnel mpls traffic-eng auto-bw** command supersedes the previous one. Therefore, if you want to specify multiple arguments for a tunnel, you must specify them all in a single **tunnel mpls traffic-eng auto-bw** command.

**Note**

Keywords for the **tunnel mpls traffic-eng auto-bw** command are order-dependent; you must enter them in the order in which they are listed in the command format.

Examples

The following example shows how to enable automatic bandwidth adjustment for tunnel102 and specify that the adjustments are to occur every hour:

```
Router(config)# interface tunnel102
Router(config-if)# tunnel mpls traffic-eng auto-bw frequency 3600
```

Related Commands

Command	Description
mpls traffic-eng auto-bw timers	Enables automatic bandwidth adjustment on a platform for tunnels configured for bandwidth adjustment.
tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for traffic engineering.

tunnel mpls traffic-eng autoroute announce

To specify that the Interior Gateway Protocol (IGP) should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation, use the **tunnel mpls traffic-eng autoroute announce** command in interface configuration mode. To disable this feature, use the **no** form of this command.

tunnel mpls traffic-eng autoroute announce

no tunnel mpls traffic-eng autoroute announce

Syntax Description This command has no arguments or keywords.

Defaults The IGP does not use the tunnel in its enhanced SPF calculation.

Command Modes Interface configuration

Command History	Release	Modification
	12.0(5)S	This command was introduced.

Usage Guidelines Currently, the only way to forward traffic onto a tunnel is by enabling this feature or by explicitly configuring forwarding (for example, with an interface static route).

Examples The following example shows how to specify that the IGP should use the tunnel in its enhanced SPF calculation if the tunnel is up:

```
Router(config-if)# tunnel mpls traffic-eng autoroute announce
```

The following example shows how to specify that if the IGP is using this tunnel in its enhanced SPF calculation, the IGP should give it an absolute metric of 10:

```
Router(config-if)# tunnel mpls traffic-eng autoroute announce metric absolute 10
```

Related Commands	Command	Description
	ip route	Establishes static routes.
	tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for traffic engineering.

tunnel mpls traffic-eng autoroute metric

To specify the Multiprotocol Label Switching (MPLS) traffic engineering tunnel metric that the Interior Gateway Protocol (IGP) enhanced shortest path first (SPF) calculation uses, use the **tunnel mpls traffic-eng autoroute metric** command in interface configuration mode. To disable the specified MPLS traffic engineering tunnel metric, use the **no** form of this command.

tunnel mpls traffic-eng autoroute metric { **absolute** | **relative** } *value*

no tunnel mpls traffic-eng autoroute metric

Syntax Description	absolute	Absolute metric mode; you can enter a positive metric value.
	relative	Relative metric mode; you can enter a positive, negative, or zero value.
	<i>value</i>	The metric that the IGP enhanced SPF calculation uses. The relative value can be from -10 to 10.
		Note Even though the value for a relative metric can be from -10 to 10, configuring a tunnel metric with a negative value is considered a misconfiguration. If from the routing table the metric to the tunnel tail appears to be 4, then the cost to the tunnel tail router is actually 3 because 1 is added to the cost for getting to the loopback address. In this instance, the lowest value that you can configure for the relative metric is -3.

Defaults The default is metric relative 0.

Command Modes Interface configuration

Command History	Release	Modification
	12.0(5)S	This command was introduced.

Examples The following example shows how to specify the use of MPLS traffic engineering tunnel metric negative 1 for the IGP enhanced SPF calculation:

```
Router(config-if)# tunnel mpls traffic-eng autoroute metric relative -1
```

Related Commands	Command	Description
	show mpls traffic-eng autoroute	Shows the tunnels announced to IGP, including interface, destination, and bandwidth.
	tunnel mpls traffic-eng autoroute announce	Instructs the IGP to use the tunnel (if it is up) in its enhanced SPF calculation.

tunnel mpls traffic-eng bandwidth

To configure bandwidth required for a Multiprotocol Label Switching (MPLS) traffic engineering tunnel, use the **tunnel mpls traffic-eng bandwidth** command in interface configuration mode. To disable this bandwidth configuration, use the **no** form of this command.

tunnel mpls traffic-eng bandwidth [**sub-pool** | **global**] *bandwidth*

no tunnel mpls traffic-eng bandwidth [**sub-pool** | **global**] *bandwidth*

Syntax Description		
	sub-pool	(Optional) Indicates a subpool tunnel.
	global	(Optional) Indicates a global pool tunnel. Entering this keyword is not necessary, for all tunnels are global pool in the absence of the sub-pool keyword. But if users of pre-DiffServ-aware Traffic Engineering (DS-TE) images enter this keyword, it is accepted.
	<i>bandwidth</i>	Bandwidth, in kilobits per second, set aside for the MPLS traffic engineering tunnel. Range is between 1 and 4294967295.

Defaults	
	Default bandwidth is 0. Default is a global pool tunnel.

Command Modes	
	Interface configuration

Command History	Release	Modification
	12.0(5)S	This command was introduced.
	12.0(11)ST	The sub-pool keyword was added.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines	
	Enter the bandwidth for either a global pool or subpool tunnel, not both. Only the ip rsvp bandwidth command specifies the two bandwidths within one command.
	To set up only a global pool tunnel, leave out the keyword sub-pool . If you enter global as a keyword, the system will accept it, but won't write it to NVRAM. This is to avoid the problem of having your configuration not understood if you upgrade to an image that contains the DS-TE capability and then return to a non-DS-TE image.

Examples	
	The following example shows how to configure 100 kbps of bandwidth for the MPLS traffic engineering tunnel:
	<pre>Router(config-if)# tunnel mpls traffic-eng bandwidth 100</pre>

Related Commands

Command	Description
show mpls traffic-eng tunnel	Displays information about tunnels.

tunnel mpls traffic-eng load-share

To determine load-sharing among two or more Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels that begin at the same router and go to an identical destination, use the **tunnel mpls traffic-eng load-share** command in interface configuration mode. To disable this feature, use the **no** form of this command.

tunnel mpls traffic-eng load-share *value*

no tunnel mpls traffic-eng load-share *value*

Syntax Description	<i>value</i>	A value from which the head-end router will calculate the proportion of traffic to be sent down each of the parallel tunnels. Range is between 1 and 1000000.
---------------------------	--------------	---

Defaults	No default behavior or values.
-----------------	--------------------------------

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

Command History	Release	Modification
	12.1(3)T	This command was introduced.

Usage Guidelines Each parallel tunnel must be configured with this command. Specify a value to indicate the *proportion* of total traffic you want to be allocated into each individual tunnel. For example, if there are to be three parallel tunnels, and you want Tunnel1 to carry half of the traffic and the other two tunnels to carry one-quarter, you should enter the following values:

- Tunnel1 -- 2
- Tunnel2 -- 1
- Tunnel3 -- 1

The ability to divide bandwidth in unequal amounts across traffic engineering tunnels has a finite granularity. This granularity varies by platform, with both hardware and software limits. If load-sharing is configured so that it exceeds the available granularity, the following message is displayed:

```
@FIB-4-UNEQUAL: Range of unequal path weightings too large for prefix x.x.x.x/y. Some available paths may not be used.
```

To eliminate this message, it is recommended that you change the requested bandwidth or load-share.

Examples

In the following example, three tunnels are configured, with the first tunnel receiving half of the traffic and the other two tunnels receiving one-quarter:

```
interface Tunnel1
  ip unnumbered Loopback0
  no ip directed-broadcast
  tunnel destination 41.41.41.41
  tunnel mode mpls traffic-eng
  tunnel mpls traffic-eng path-option 10 dynamic
  tunnel mpls traffic-eng load-share 2

interface Tunnel2
  ip unnumbered Loopback0
  no ip directed-broadcast
  tunnel destination 41.41.41.41
  tunnel mode mpls traffic-eng
  tunnel mpls traffic-eng path-option 10 dynamic
  tunnel mpls traffic-eng load-share 1

interface Tunnel3
  ip unnumbered Loopback0
  no ip directed-broadcast
  tunnel destination 41.41.41.41
  tunnel mode mpls traffic-eng
  tunnel mpls traffic-eng path-option 10 dynamic
  tunnel mpls traffic-eng load-share 1
```

Related Commands

Command	Description
show ip route	Displays routing table information about tunnels, including their traffic share.
tunnel mpls traffic-eng bandwidth	Configures bandwidth in Kbps for an MPLS traffic engineering tunnel.

tunnel mpls traffic-eng path-option

To configure a path option for a Multiprotocol Label Switching (MPLS) traffic engineering tunnel, use the **tunnel mpls traffic-eng path-option** command in interface configuration mode. To disable the specified path option, use the **no** form of this command.

```
tunnel mpls traffic-eng path-option number { dynamic | explicit { name path-name | path-number } } [lockdown]
```

```
no tunnel mpls traffic-eng path-option number { dynamic | explicit { name path-name | path-number } } [lockdown]
```

Syntax Description

<i>number</i>	When multiple path options are configured, lower numbered options are preferred.
dynamic	Path of the LSP is dynamically calculated.
explicit	Path of the LSP is an IP explicit path.
name <i>path-name</i>	Path name of the IP explicit path that the tunnel uses with this option.
<i>path-number</i>	Path number of the IP explicit path that the tunnel uses with this option.
lockdown	(Optional) The LSP cannot be reoptimized.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines

You can configure multiple path options for a single tunnel. For example, there can be several explicit path options and a dynamic option for one tunnel. Path setup preference is for lower (not higher) numbers, so option 1 is preferred.

Examples

The following example shows how to configure the tunnel to use a named IP explicit path:

```
Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit name test
```

Related Commands

Command	Description
ip explicit-path	Enters the subcommand mode for IP explicit paths and creates or modifies the specified path.

Command	Description
show ip explicit-paths	Displays the configured IP explicit paths.
tunnel mpls traffic-eng priority	Configures the setup and reservation priority for an MPLS traffic engineering tunnel.

tunnel mpls traffic-eng priority

To configure the setup and reservation priority for an Multiprotocol Label Switching (MPLS) traffic engineering tunnel, use the **tunnel mpls traffic-eng priority** command in interface configuration mode. To remove the specified setup and reservation priority, use the **no** form of this command.

tunnel mpls traffic-eng priority *setup-priority* [*hold-priority*]

no tunnel mpls traffic-eng priority *setup-priority* [*hold-priority*]

Syntax Description

<i>setup-priority</i>	The priority used when signalling an LSP for this tunnel to determine which existing tunnels can be preempted. Valid values are from 0 to 7, where a lower number indicates a higher priority. Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non-0 priority.
<i>hold-priority</i>	(Optional) The priority associated with an LSP for this tunnel to determine if it should be preempted by other LSPs that are being signalled. Valid values are from 0 to 7, where a lower number indicates a higher priority.

Defaults

setup-priority: 7
hold-priority: The same value as the *setup-priority*

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines

When a label switched path (LSP) is being signaled and an interface does not currently have enough bandwidth available for that LSP, the call admission software preempts lower-priority LSPs so that the new LSP can be admitted. (LSPs are preempted if that allows the new LSP to be admitted.)

In the described determination, the new LSP's priority is its setup priority and the existing LSP's priority is its hold priority. The two priorities make it possible to signal an LSP with a low setup priority (so that the LSP does not preempt other LSPs on setup) but a high hold priority (so that the LSP is not preempted after it is established).

Setup priority and hold priority are typically configured to be equal, and setup priority cannot be better (numerically smaller) than the hold priority.

Examples

The following example shows how to configure a tunnel with a setup and hold priority of 1:

```
Router(config-if)# tunnel mpls traffic-eng priority 1
```

Related Commands

Command	Description
tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for traffic engineering.

tunnel mpls traffic-eng record-route

To include the interface address for the label switched path (LSP) in the Record Route Object (RRO) for an RESV message, use the **tunnel mpls traffic-eng record-route** command in interface configuration mode. To remove the interface address for the LSP in the RRO for the RESV message, use the **no** form of this command.

tunnel mpls traffic-eng record-route

no tunnel mpls traffic-eng record-route

Syntax Description This command has no arguments or keywords.

Command Default By default, this command is disabled. The interface addresses for the LSP are not included in the RRO of the RESV message. The **record-route** option is automatically enabled when the **tunnel mpls traffic-eng fast-reroute** command for the fast-reroute (FRR) feature is enabled at the headend.

Command Modes Interface configuration

Command History	Release	Modification
	12.0(5)S	This command was introduced.
	12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines The RRO has two functions. It records the route of the LSP that can be used in loop prevention, and it records labels that are used by FRR.

The contents of a RRO are a series of variable-length data items called subobjects.

If record route is enabled, the RRO contains details in the following order: node-ID, interface address, and label.

Examples The following example shows how to include the interface address using the **tunnel mpls traffic-eng record-route** command:

```
interface tunnel1
ip unnumbered loopback0
no ip direct-broadcast
tunnel destination 192.168.1.5
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng bandwidth 100
tunnel mpls traffic-eng priority 1 1
tunnel mpls traffic-eng path-option 1 dynamic
tunnel mpls traffic-eng record-route
```

Related Commands,	Command	Description
	show ip rsvp reservation	Displays current RSVP related receiver information in the database.
	show mpls traffic-eng tunnels	Displays information on the source, destination, path and interface of MPLS TE tunnels.
	tunnel mpls traffic-eng fast-reroute	Enables an MPLS TE tunnel to use an established backup tunnel in the event of a link or node failure.

tunnel tsp-hop

To define hops in the path for the label switching tunnel, use the **tunnel tsp-hop** command in interface configuration mode. To remove these hops, use the **no** form of this command.

tunnel tsp-hop *hop-number ip-address [lasthop]*

no tunnel tsp-hop *hop-number ip-address [lasthop]*

Syntax Description		
	<i>hop-number</i>	The sequence number of the hop being defined in the path. The first number is 1, which identifies the hop just after the head hop.
	<i>ip-address</i>	The IP address of the input interface on that hop.
	lasthop	(Optional) Indicates that the hop being defined is the final hop in the path (the tunnel destination).

Defaults No hops are defined.

Command Modes Interface configuration

Command History	Release	Modification
	11.1 CT	This command was introduced.

Usage Guidelines The list of tunnel hops must specify a strict source route for the tunnel. In other words, the router at hop <n> must be directly connected to the router at hop <n>+1.

Examples The following example shows how to configure a two-hop tunnel. The first hop router/switch is 172.16.0.2, and the second and last hop is router/switch 172.17.0.2.

```
Router(config)# interface tunnel 5

Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# ip unnumbered e0/1
Router(config-if)# tunnel tsp-hop 1 172.16.0.2
Router(config-if)# tunnel tsp-hop 2 172.17.0.2 lasthop
```

Related Commands	Command	Description
	tunnel mpls traffic-eng affinity	Sets the encapsulation mode of the tunnel to label switching.

vlan database

To enter virtual LAN (VLAN) configuration mode, use the **vlan database** command in privileged EXEC mode.

vlan database

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(7)XE	This command was introduced on the Catalyst 6000 family switches.
	12.1(1)E	Support for this command on the Catalyst 6000 family switches was extended to the E train.
	12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines Once you are in VLAN configuration mode, you can access the VLAN database editing buffer manipulation commands, including:

- **abort**—Used to exit mode without applying the changes.
- **apply**—Used to apply current changes and bump revision number.
- **exit**—Used to apply changes, bump revision number, and exit mode.
- **no**—Used to negate a command or set its defaults; valid values are **vlan** and **vtp**.
- **reset**—Used to abandon current changes and reread current database.
- **show**—Used to display database information.
- **vlan**—Used to access subcommands to add, delete, or modify values associated with a single VLAN. For information about the **vlan** subcommands, see the **vlan** (VLAN configuration mode) command.
- **vtp**—Used to access subcommands to perform Virtual Terminal Protocol (VTP) administrative functions. For information about the **vtp** subcommands, see the **vtp client** command.

Examples

The following example shows how to enter VLAN configuration mode:

```
Router# vlan database  
Router(vlan)#
```

The following example shows how to exit VLAN configuration mode without applying changes after you are in VLAN configuration mode:

```
Router(vlan)# abort  
Aborting....  
Router#
```

The following example shows how to delete a VLAN after you are in VLAN configuration mode:

```
Router(vlan)# no vlan 100  
Deleting VLAN 100...  
Router(vlan)#
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

vlan (VLAN configuration mode)

To configure a specific virtual LAN (VLAN), use the **vlan** command in VLAN configuration mode. To delete a VLAN, use the **no** form of this command without additional options.

```
vlan vlan-id [are hops] [backupcrf mode] [bridge type | bridge-number] [media type] [mtu
mtu-size] [name vlan-name] [parent parent-vlan-id] [ring ring-number] [said sa-id-value]
[state {suspend | active}] [stp type type] [tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]
```

```
no vlan
```

Syntax	Description
<i>vlan-id</i>	Number of the VLAN; valid values are from 2 to 1001.
are <i>hops</i>	(Optional) Specifies the maximum number of All Route Explorer hops for this VLAN. Valid values are from 0 to 13. Zero is assumed if no value is specified.
backupcrf <i>mode</i>	(Optional) Enables or disables the backup concentrator relay function (CRF) mode of the VLAN; valid values are enable or disable .
bridge <i>type</i> <i>bridge-number</i>	(Optional) Specifies the bridging characteristics of the VLAN or identification number of the bridge; valid type values are srb or srt . Valid <i>bridge-number</i> values are from 0 to 15.
media <i>type</i>	(Optional) Specifies the media type of the VLAN; valid values are ethernet , fd-net , fdi , trcrf , and trbrf .
mtu <i>mtu-size</i>	(Optional) Specifies the maximum transmission unit (packet size, in bytes) that the VLAN can use; valid values are from 576 to 18190.
name <i>vlan-name</i>	(Optional) Defines a text string used as the name of the VLAN (1 to 32 characters).
parent <i>parent-vlan-id</i>	(Optional) Specifies the ID number of the parent VLAN of FDDI or Token Ring-type VLANs; valid values are from 2 to 1001.
ring <i>ring-number</i>	(Optional) Specifies the ring number of FDDI or Token Ring-type VLANs; valid values are from 2 to 1001.
said <i>sa-id-value</i>	(Optional) Specifies the security association identifier; valid values are from 1 to 4294967294
state { suspend active }	(Optional) Specifies whether the state of the VLAN is active or suspended. VLANs in suspended state do not pass packets.
stp <i>type</i> <i>type</i>	(Optional) Specifies the Spanning Tree Protocol (STP) type; valid values are ieee , ibm , and auto .
tb-vlan1 <i>tb-vlan1-id</i>	(Optional) Specifies the ID number of the first translational VLAN for this VLAN; valid values are from 2 to 1001. Zero is the default value.
tb-vlan2 <i>tb-vlan2-id</i>	(Optional) Specifies the ID number of the second translational VLAN for this VLAN; valid values are from 2 to 1001. Zero is the default value.

Defaults

The defaults are as follows:

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

media type—ethernet

state—active

said-value—100000 plus the VLAN ID number

mtu-size—dependent upon the VLAN type:

- ethernet—1500
- fddi—1500
- trcrf—1500 if V2 is not enabled, 4472 if it is enabled
- fd-net—1500
- trbrf—1500 if V2 is not enabled, 4472 if it is enabled

ring-number—no ring number is specified

bridge-number—no bridge number is specified

parent-vlan-id—no parent VLAN is specified

type—no STP type is specified

tb-vlan1 and **tb-vlan2**—0, which means no translational bridge VLAN is specified

Command Modes

VLAN configuration

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 family switches.
12.1(1)E	Support for this command on the Catalyst 6000 family switch was extended to the E train.
12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

VLAN 1 parameters are factory configured and cannot be changed.

When you define *vlan-name*, the name must be unique within the administrative domain.

The Security association ID (SAID) is documented in 802.10. When the **no** form is used, the VLAN's SAID is returned to the default.

When you define the *said-value*, the name must be unique within the administrative domain.

The *bridge-number* argument is used only for Token Ring-net and FDDI-net VLANs and is ignored in other types of VLANs. When the **no** form is used, the VLAN's source-routing bridge number returns to the default.

The parent VLAN resets to the default if the parent VLAN is deleted or the media keyword changes the VLAN type or the VLAN type of the parent VLAN.

The **tb-vlan1** and **tb-vlan2** keywords are used to configure translational bridge VLANs of a specified type of VLAN and are not allowed in other types of VLANs. Translational bridge VLANs must be of a differing VLAN type as the affected VLAN; if two VLANs are specified, the two must be of differing VLAN types.

A translational bridge VLAN will reset to the default if the translational bridge VLAN is deleted or the media keyword changes the VLAN type or the VLAN type of the corresponding translational bridge VLAN.

Examples

The following example shows how to add a new VLAN with all default parameters to the new VLAN database:

```
Router(vlan)# vlan 2
```



Note

If the VLAN already exists, no action occurs.

The following example shows how to cause the device to add a new VLAN, specify the media type and parent VLAN ID number 3, and set all other parameters to the defaults:

```
Router(vlan)# vlan 2 media ethernet parent 3
```

```
VLAN 2 modified:
  Media type ETHERNET
  Parent VLAN 3
```

The following example shows how to delete VLAN 2:

```
Router(vlan)# no vlan 2
```

The following example shows how to return the maximum transmission unit (MTU) to the default for its type and return translational bridging VLANs to the default:

```
Router(vlan)# no vlan 2 mtu tb-vlan1 tb-vlan2
```

Related Commands

Command	Description
show vlan	Displays VLAN information.
vlan database	Enters VLAN configuration mode.

vpn id

To set or update a Virtual Private Network (VPN) ID on a VPN routing/forwarding instance (VRF), use the **vpn id** command in VRF configuration mode. To remove the VPN ID from the VRF, use the **no** form of this command.

vpn id *oui:vpn-index*

no vpn id [*oui:vpn-index*]

Syntax Description

<i>oui</i>	Organizationally unique identifier. The IEEE organization assigns this identifier to companies. The OUI is restricted to three octets.
<i>vpn-index</i>	Identifies the VPN within the company. This VPN index is restricted to four octets.

Defaults

The VPN ID is not set.

Command Modes

VRF configuration

Command History

Release	Modification
12.0(17)ST	This command was introduced.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Each VRF configured in a provider edge (PE) router can have a VPN ID. Use the same VPN ID for the PE routers that belong to the same VPN. Make sure the VPN ID is unique for each VPN in the service provider network.

To change the VPN ID, issue the command again. The new ID overwrites the old one.

Examples

The following example shows how to assign the VPN ID of 0000a100003f6c to a VRF called vpn1:

```
Router(config)# ip vrf vpn1
Router(config-vrf)# vpn id a1:3f6c
```

Related Commands

Command	Description
show ip vrf detail	Displays all the VRFs on a router.
show ip vrf id	Displays all the VPN IDs that are configured in the router and their associated VRF names and VRF route distinguishers (RDs).

vtp client

To place the device in VLAN Trunking Protocol (VTP) client mode, use the **vtp client** command in virtual LAN (VLAN) configuration mode. To return to VTP server mode, use the **no** form of this command.

vtp client

no vtp client

Syntax Description This command has no arguments or keywords.

Defaults Server mode

Command Modes VLAN configuration

Command History	Release	Modification
	12.0(7)XE	This command was introduced on the Catalyst 6000 family switches.
	12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines 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.

The **vtp server** command is the functional equivalent of **no vtp client** command except that it does not return an error if the device is not in client mode.

Examples The following example shows how to place the device in VTP client mode:

```
Router(vlan)# vtp client
```

Related Commands	Command	Description
	show vtp	Displays VTP statistics and domain information.
	vtp (global configuration)	Modifies the name of the VTP configuration storage file.
	vtp server	Places a device in VTP server mode.
	vtp transparent	Places a device in VTP transparent mode.

vtp domain

To configure the administrative domain name for the device, use the **vtp domain** command in virtual LAN (VLAN) configuration mode.

vtp domain *domain-name*

Syntax Description

<i>domain-name</i>	Domain name.
--------------------	--------------

Defaults

This command has no default setting.

Command Modes

VLAN configuration

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 family switches.
12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

When you define the *domain-name* argument, the domain name is case sensitive.

Until a domain name is set, the device is in the no-management-domain state. In this state, the device does not transmit any VLAN Trunking Protocol (VTP) advertisements regardless of changes to local VLAN configuration. The device leaves the no-management-domain state upon receiving the first VTP summary packet on any port that is currently trunking or upon configuration of a domain name using the **vtp domain** command. If the device receives its domain from a summary packet, it resets its configuration revision number to zero.

Once the device leaves the no-management-domain state, it can never be configured to reenter it, except by cleaning NVRAM and reloading.

Examples

The following example shows how to set the device's administrative domain:

```
Router(vlan)# vtp domain DomainChandon
```

Related Commands

Command	Description
show vtp	Displays VTP statistics and domain information.
vtp (global configuration)	Modifies the name of the VTP configuration storage file.

vtp password

To create a VLAN Trunking Protocol (VTP) domain password, use the **vtp password** command in virtual LAN (VLAN) configuration mode. To delete the password, use the **no** form of this command.

vtp password *password-value*

no vtp password

Syntax Description	<i>password-value</i>	Specifies the password. The value is an ASCII string from 1 to 32 characters identifying the administrative domain for the device.
---------------------------	-----------------------	--

Defaults	The default is no password.
-----------------	-----------------------------

Command Modes	VLAN configuration
----------------------	--------------------

Command History	Release	Modification
	12.0(7)XE	This command was introduced on the Catalyst 6000 family switches.
	12.1(1)E	Support for this command on the Catalyst 6000 family switches was extended to the E train.
	12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines	The value of the <i>password-value</i> argument is an ASCII string from 1 to 32 characters identifying the administrative domain for the device.
-------------------------	--

Examples The following example shows how to create a VTP domain password:

```
Router(vlan)# vtp password DomainChandon
```

The following example shows how to delete the VTP domain password:

```
Router(vlan)# no vtp password
Clearing device VLAN database password.
```

Related Commands	Command	Description
	show vtp	Displays VTP statistics and domain information.
	vtp (global configuration)	Modifies the name of the VTP configuration storage file.

vtp server

To place the device in VLAN Trunking Protocol (VTP) server mode, use the **vtp server** command in virtual LAN (VLAN) configuration mode.

vtp server

Syntax Description This command has no arguments or keywords.

Defaults The default is VTP server mode.

Command Modes VLAN configuration

Command History	Release	Modification
	12.0(7)XE	This command was introduced on the Catalyst 6000 family switches.
	12.1(1)E	Support for this command on the Catalyst 6000 family switches was extended to the E train.
	12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

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.

VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.

If the receiving switch is in server mode, the configuration is not changed.

The **vtp server** command is the functional equivalent of **no vtp client** command except that it does not return an error if the device is not in client mode.

Examples The following example shows how to place the device in VTP server mode:

```
Router(vlan)# vtp server
```

Related Commands	Command	Description
	show vtp	Displays VTP statistics and domain information.
	vtp (global configuration)	Modifies the name of the VTP configuration storage file.
	vtp client	Places a device in VTP client mode.
	vtp transparent	Places a device in VTP transparent mode.

vtp transparent

To place the device in VLAN Trunking Protocol (VTP) transparent mode, use the **vtp transparent** command in virtual LAN (VLAN) configuration mode. To return to VTP server mode, use the **no** form of this command.

vtp transparent

no vtp transparent

Syntax Description This command has no arguments or keywords.

Defaults The default is VTP server mode.

Command Modes VLAN configuration

Command History	Release	Modification
	12.0(7)XE	This command was introduced on the Catalyst 6000 family switches.
	12.1(1)E	Support for this command on the Catalyst 6000 family switches was extended to the E train.
	12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines The **vtp transparent** command disables VTP from the domain but does not remove the domain from the switch.

If the receiving switch is in transparent mode, the 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 the other switches in the network.

The **vtp server** command is similar to the **no vtp transparent** command, except that it does not return an error if the device is not in transparent mode.

Examples The following example shows how to place the device in VTP transparent mode:

```
Router(vlan)# vtp transparent
```

The following example shows how to return the device to VTP server mode:

```
Router(vlan)# no vtp transparent
```

Related Commands	Command	Description
	show vtp	Displays VTP statistics and domain information.
	vtp (global configuration)	Modifies the name of the VTP configuration storage file.
	vtp client	Places a device in VTP client mode.
	vtp server	Places a device in VTP server mode.

vtp v2-mode

To enable VLAN Trunk Protocol (VTP) version 2 mode, use the **vtp v2-mode** command in virtual LAN (VLAN) configuration mode. To disable version 2 mode, use the **no** form of this command.

vtp v2-mode

no vtp v2-mode

Syntax Description This command has no arguments or keywords.

Defaults Version 2 mode is disabled.

Command Modes VLAN configuration

Command History	Release	Modification
	12.0(7)XE	This command was introduced on the Catalyst 6000 family switches.
	12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1) E on the Catalyst 6000 family switches.
	12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines All switches in a VTP domain must run the same version of VTP. VTP version 1 and VTP version 2 do not operate on switches in the same VTP domain.

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

If you toggle the version 2 mode, parameters of certain default VLANs are modified.

Examples The following example shows how to enable version 2 mode in the VLAN database:

```
Router(vlan)# vtp v2-mode
```

The following example shows how to disable version 2 mode in the VLAN database:

```
Router(vlan)# no vtp v2-mode
```

Related Commands	Command	Description
	show vtp	Displays VTP statistics and domain information.
	vtp (global configuration)	Modifies the name of the VTP configuration storage file.