

mac-address-table aging-time

To configure the maximum aging time for entries in the Layer 2 table, use the **mac-address-table aging-time** command in global configuration mode. To reset the seconds value to the default setting, use the **no** form of this command.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

mac-address-table aging-time *seconds*

no mac-address-table aging-time *seconds*

Catalyst Switches

mac-address-table aging-time *seconds* [**vlan** *vlan-id*]

no mac-address-table aging-time *seconds* [**vlan** *vlan-id*]

Syntax Description		
<i>seconds</i>		MAC address table entry maximum age. Valid values are 0, and from 10 to 1000000 seconds. Aging time is counted from the last time that the switch saw the mac-address. The default value is 300 seconds
vlan <i>vlan-id</i>		(Optional) Specifies the VLAN to apply the changed aging time; valid values are from 2 to 1001.

Command Default The system uses a default of 300 seconds for the mac-address-table aging-time when the **mac-address-table aging-time** command has not been configured.

Command Modes Global configuration

Command History	Release	Modification
	12.0(7)XE	This command was introduced on Catalyst 6000 family switches.
	12.1(1)E	This command was implemented on Catalyst 6000 family switches.
	12.2(2)XT	This command was introduced on 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 Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The aging time entry will take the specified value. Valid entries are from 10 to 1,000,000 seconds. This command cannot be disabled.

Catalyst Switches

If you do not enter a VLAN, the change is applied to all routed-port VLANs.

Enter 0 seconds to disable aging.

Examples

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The following example shows the aging time being configured:

```
Router(config)# mac-address-table aging-time 300
```

Catalyst Switches

The following example shows the aging time being configured:

```
Router(config)# mac-address-table aging-time 400
```

The following example shows the aging time being disabled:

```
Router(config)# mac-address-table aging-time 0
```

Related Commands

Command	Description
<code>show mac-address-table aging-time</code>	Displays the MAC address aging time.

mac-address-table dynamic

To add dynamic addresses to the MAC address table, use the **mac-address-table dynamic** command in global configuration mode. Dynamic addresses are automatically added to the address table and dropped from it when they are not in use. To remove dynamic entries from the MAC address table, use the **no** form of this command.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

mac-address-table dynamic *hw-address* interface {**fa** | **gi**} [*slot/port*] **vlan** *vlan-id*

no mac-address-table dynamic *hw-address* **vlan** *vlan-id*

Catalyst Switches

mac-address-table dynamic *hw-address* interface [**atm** *slot/port*] [**vlan** *vlan-id*]

no mac-address-table dynamic *hw-address* [**vlan** *vlan-id*]

Syntax Description		
<i>hw-address</i>		MAC address added to or removed from the table.
<i>interface</i>		Port to which packets destined for <i>hw-address</i> are forwarded.
fa		Specifies FastEthernet.
gi		Specifies GigabitEthernet.
<i>slot</i>		(Optional) The slot (slot 1 or slot 2) to which to add dynamic addresses.
<i>port</i>		(Optional) Port interface number. The ranges are based on type of Ethernet switch network module used: 0 to 15 for NM-16ESW 0 to 35 for NM-36ESW 0 to 1 for GigabitEthernet
atm <i>slot/port</i>		(Optional) Add dynamic addresses to the ATM module in slot 1 or 2. The port is always 0 for an ATM interface.

vlan *vlan-id*

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The interface and **vlan** parameters together specify a destination to which packets destined for *hw-address* are forwarded.

The **vlan** keyword is optional if the port is a static-access or dynamic-access VLAN port. In this case, the VLAN assigned to the port is assumed to be that of the port associated with the MAC address.

The **vlan** keyword is required for multi-VLAN and trunk ports. This keyword is required on trunk ports to specify to which VLAN the dynamic address is assigned.

The *vlan-id* is the value of the ID of the VLAN to which packets destined for *hw-address* are forwarded. Valid IDs are 1 to 1005; do not enter leading zeroes.

Catalyst Switches

(Optional) The interface and **vlan** parameters together specify a destination to which packets destined for *hw-address* are forwarded.

The **vlan** keyword is optional if the port is a static-access or dynamic-access VLAN port. In this case, the VLAN assigned to the port is assumed to be that of the port associated with the MAC address.

Note When this command is executed on a dynamic-access port, queries to the VLAN Membership Policy Server (VMPS) do not occur. The VMPS cannot verify that the address is allowed or determine to which VLAN the port should be assigned. This command should be used only for testing purposes.

The **vlan** keyword is required for multi-VLAN and trunk ports. This keyword is required on trunk ports to specify to which VLAN the dynamic address is assigned.

The *vlan-id* is the value of the ID of the VLAN to which packets destined for *hw-address* are forwarded. Valid IDs are 1 to 1005; do not enter leading zeroes.

Defaults

Dynamic addresses are not added to the MAC address table.

Command Modes

Global configuration

Command History

Release	Modification
11.2(8)SA	This command was first introduced.
11.2(8)SA3	The vlan keyword was added.
11.2(8)SA5	The atm keyword was added.
12.2(2)XT	This command was implemented on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T, on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

If the *vlan-id* argument is omitted and the **no** form of the command is used, the MAC address is removed from all VLANs.

Examples

The following example shows how to add a MAC address on port fa1/1 to VLAN 4:

```
Switch(config)# mac-address-table dynamic 00c0.00a0.03fa fa1/1 vlan 4
```

Related Commands

Command	Description
clear mac-address-table	Deletes entries from the MAC address table.
mac-address-table aging-time	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.
mac-address-table static	Adds static addresses to the MAC address table.
show mac-address-table	Displays the MAC address table.

mac-address-table secure

To add secure addresses to the MAC address table, use the **mac-address-table secure** command in global configuration mode. To remove secure entries from the MAC address table, use the **no** form of this command.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

```
mac-address-table secure hw-address interface {fa | gi} slot/port vlan vlan-id
```

```
no mac-address-table secure hw-address vlan vlan-id
```

Catalyst Switches

```
mac-address-table secure hw-address interface [atm slot/port] [vlan vlan-id]
```

```
no mac-address-table secure hw-address [vlan vlan-id]
```

Syntax Description		
<i>hw-address</i>		MAC address that is added to the table.
<i>interface</i>		Port to which packets destined for <i>hw-address</i> are forwarded.
fa		Specifies FastEthernet.
gi		Specifies Gigabit Ethernet.
<i>slot</i>		(Optional) The slot (slot 1 or slot 2) to which to add dynamic addresses.
<i>port</i>		(Optional) Port interface number. The ranges are based on type of Ethernet switch network module used: 0 to 15 for NM-16ESW 0 to 35 for NM-36ESW 0 to 1 for GigabitEthernet
atm slot/port		(Optional) Add secure address to the ATM module in slot 1 or 2. The port is always 0 for an ATM interface.

vlan *vlan-id***Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers**

The *interface* and **vlan** parameters together specify a destination to which packets destined for *hw-address* are forwarded.

The **vlan** keyword is optional if the port is a static-access VLAN port. In this case, the VLAN assigned to the port is assumed to be that of the port associated with the MAC address. This keyword is required for multi-VLAN and trunk ports.

The value of *vlan-id* is the ID of the VLAN to which secure entries are added. Valid IDs are 1 to 1005; do not enter leading zeroes.

Catalyst Switches

(Optional) The *interface* and **vlan** parameters together specify a destination to which packets destined for *hw-address* are forwarded.

The **vlan** keyword is optional if the port is a static-access VLAN port. In this case, the VLAN assigned to the port is assumed to be that of the port associated with the MAC address. This keyword is required for multi-VLAN and trunk ports.

The value of *vlan-id* is the ID of the VLAN to which secure entries are added. Valid IDs are 1 to 1005; do not enter leading zeroes.

Defaults

Secure addresses are not added to the MAC address table.

Command Modes

Global configuration

Command History

Release	Modification
11.2(8)SA	This command was first introduced.
11.2(8)SA3	The vlan keyword was added.
11.2(8)SA5	The atm keyword was added.
12.2(2)XT	This command was implemented on 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 Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines**Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers**

Secure addresses can be assigned to only one port at a time. Therefore, if a secure address table entry for the specified MAC address and VLAN already exists on another port, it is removed from that port and assigned to the specified one.

Catalyst Switches

Secure addresses can be assigned only to one port at a time. Therefore, if a secure address table entry for the specified MAC address and VLAN already exists on another port, it is removed from that port and assigned to the specified one.

Dynamic-access ports cannot be configured with secure addresses.

Examples**Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers**

The following example shows how to add a secure MAC address to VLAN 6 of port fa1/1:

```
Router(config)# mac-address-table secure 00c0.00a0.03fa fa1/1 vlan 6
```

Catalyst Switches

The following example shows how to add a secure MAC address to VLAN 6 of port fa1/1:

```
Switch(config)# mac-address-table secure 00c0.00a0.03fa fa1/1 vlan 6
```

The following example shows how to add a secure MAC address to ATM port 2/1:

```
Switch(config)# mac-address-table secure 00c0.00a0.03fa atm 2/1
```

Related Commands

Command	Description
clear mac-address-table	Deletes entries from the MAC address table.
mac-address-table aging-time	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.
mac-address-table dynamic	Adds dynamic addresses to the MAC address table.
mac-address-table static	Adds static addresses to the MAC address table.
show mac-address-table	Displays the MAC address table.

mac-address-table static

To add static entries to the MAC address table, use the **mac-address-table static** command in global configuration mode. To remove entries profiled by the combination of specified entry information, use the **no** form of this command.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

```
mac-address-table static mac-address {vlan vlan-id} {interface type slot/port}
```

```
no mac-address-table static mac-address {vlan vlan-id} {interface type slot/port}
```

Catalyst Switches

```
mac-address-table static mac-address {vlan vlan-id} {interface int} [protocol {ip | ipx | assigned}]
```

```
no mac-address-table static mac-address {vlan vlan-id} {interface int} [protocol {ip | ipx | assigned}]
```

Syntax Description		
<i>mac-address</i>		Address to add to the MAC address table.
vlan <i>vlan-id</i>		(Optional) Specifies the VLAN associated with the MAC address entry; valid values are from 2 to 100.
interface <i>type slot/port</i>		Specifies the interface type and the slot and port configured.
protocol		(Optional) Specifies the protocol associated with the entry.
ip		Specifies the IP protocol.
ipx		Specifies the IPX protocol.
assigned		Specifies assigned protocol bucket accounts for such protocols as DECnet, Banyan VINES, and AppleTalk.

Defaults Static entries are not added to the MAC address table.

Command Modes Global configuration

Command History	Release	Modification
	12.0(7)XE	This command was introduced on Catalyst 6000 family switches.
	12.1(1)E	Support for this command on Catalyst 6000 family switches was extended to the E train.
	12.1(5c)EX	This command was changed to support multicast addresses.
	12.2(2)XT	This command was implemented on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(11)T	This command was integrated into Cisco IO Release 12.2(11)T.

Usage Guidelines

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The output interface specified must be a Layer 2 IDB and not an SVI.

Entering the **no** form of this command does not remove system MAC addresses.

When removing a MAC address, entering the **interface** *type slot/port* argument is optional. For unicast entries, the entry is removed automatically. For multicast entries, if you do not specify an interface, the entire entry is removed. You can specify the selected ports to be removed by specifying the interface.

Catalyst Switches

The output interface specified must be a Layer 2 IDB and not a switch virtual interface (SVI).

You can enter up to 15 interfaces per command entered, but you can enter more interfaces by repeating the command.

If you do not enter a protocol type, an entry is automatically created for each of the four protocol types.

Entering the **no** form of this command does not remove system MAC addresses.

When removing a MAC address, entering the **interface** *type slot/port* argument is optional. For unicast entries, the entry is removed automatically. For multicast entries, if you do not specify an interface, the entire entry is removed. You can specify the selected ports to be removed by specifying the interface.

Examples

The following example shows how to add static entries to the MAC address table:

```
Router(config)# mac-address-table static 0050.3e8d.6400 vlan 100 interface fastethernet5/7
```

Related Commands

Command	Description
show mac-address-table address	Displays MAC address table information for a specific MAC address.

mask destination

To specify the destination mask, use the **mask destination** command in aggregation cache configuration mode. To disable the destination mask, use the **no** form of this command.

mask destination minimum *value*

no mask destination minimum *value*

Syntax Description	minimum	Configures the minimum value for the mask.
	<i>value</i>	Specifies the configurable value for the mask. Range is from 1 to 32.

Defaults The default value of the minimum mask is zero.

Command Modes Aggregation cache configuration

Command History	Release	Modification
	12.1(2)T	This command was introduced.

Usage Guidelines This command is only available with router-based aggregation. Minimum masking capability is not available if router-based aggregation is not enabled.

Examples The following example shows how to configure the destination-prefix aggregation cache with a minimum mask value:

```
Router(config)# ip flow-aggregation cache destination-prefix
Router(config-flow-cache)# mask destination minimum 32
```

Related Commands	Command	Description
	ip flow-aggregation cache	Enables aggregation cache configuration mode.
	mask source	Specifies the source mask.
	show ip cache flow aggregation	Displays the aggregation cache configuration.

mask source

To specify the source mask, use the **mask source** command in aggregation cache configuration mode. To disable the source mask, use the **no** form of this command.

mask source minimum *value*

no mask source minimum *value*

Syntax Description

minimum	Configures the minimum value for the mask.
<i>value</i>	Specifies the configurable value for the mask. Range is from 1 to 32.

Defaults

The default value of the minimum source is zero.

Command Modes

Aggregation cache configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

This command is only available with router-based aggregation. Minimum masking capability is not available if router-based aggregation is not enabled.

Examples

The following example shows how to configure the source-prefix aggregation cache with a minimum mask value:

```
Router(config)# ip flow-aggregation cache source-prefix
Router(config-flow-cache)# mask source minimum 30
```

Related Commands

Command	Description
ip flow-aggregation cache	Enables aggregation cache configuration mode.
mask destination	Specifies the destination mask.
show ip cache flow aggregation	Displays the aggregation cache configuration.

match mpls-label

To redistribute routes that include Multiprotocol Label Switching (MPLS) labels if the routes meet the conditions specified in the route map, use the **match mpls-label** command in route map configuration mode. To disable this function, use the **no** form of this command.

match mpls-label

no match mpls-label

Syntax Description This command has no arguments or keywords.

Defaults Routes with MPLS labels are not redistributed.

Command Modes Route map configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

A route map that includes this command can be used in the following instances:

- With the **neighbor route-map in** command to manage inbound route maps in BGP
- With the **redistribute bgp** command to redistribute route maps in an IGP

Use the **route-map** global configuration command, and the **match** and **set** route map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match route-map** configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must “pass” to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Examples

The following example shows how to create a route map that redistributes routes if the following conditions are met:

- The IP address of the route matches an IP address in ACL 2.
- The route includes an MPLS label.

```
Router(config-router)# route-map incoming permit 10
Router(config-route-map)# match ip address 2
Router(config-route-map)# match mpls-label
```

Related Commands

Command	Description
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set mpls-label	Enables a route to be distributed with an MPLS label if the route matches the conditions specified in the route map.

maximum routes

To limit the maximum number of routes in a Virtual Private Network (VPN) routing/forwarding instance (VRF) to prevent a provider edge (PE) router from importing too many routes, use the **maximum routes** command in VRF configuration submode. To remove the limit on the maximum number of routes allowed, use the **no** form of this command.

maximum routes *limit* {*warn-threshold* | **warning-only**}

no maximum routes

Syntax Description		
	<i>limit</i>	Specifies the maximum number of routes allowed in a VRF. The valid range is from 1 to 4,294,967,295 routes.
	<i>warn-threshold</i>	The warning threshold value is expressed as a percentage (from 1 to 100) of the <i>limit</i> value. When the number of routes reaches the specified percentage of the limit, a warning message is generated.
	warning-only	Issues a syslog error message when the maximum number of routes allowed for a VRF exceeds the threshold. However, additional routes are still allowed.

Defaults

No limit is set on the maximum number of routes allowed.

Command Modes

VRF configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(13)T	Support for SNMP notifications was added.

Usage Guidelines

The **maximum routes** command can be configured in one of two ways:

- Generate a warning message when the *limit* is exceeded
- Generate a warning message when the *warn-threshold* is reached

To limit the number of routes allowed in the VRF, use the **maximum routes** *limit* command with the *warn-threshold* argument. The *warn-threshold* argument generates a warning and does not allow the addition of routes to the VRF when the maximum number set by the *limit* argument is reached. The software generates a warning message everytime a route is added to a VRF when the VRF route count is above the warning threshold. The software also generates a route rejection notification when the maximum threshold is reached and everytime a route is rejected after the limit is reached.

To set a number of routes at which you receive a notification, but which does not limit the number of routes that can be imported into the VRF, use the **maximum routes** *limit* command with the **warn-only** keyword.

To configure the router to generate SNMP notifications (traps or informs) for these values use the **snmp-server enable traps mpls vpn** global configuration command.

Examples

The following example shows how to set a limit threshold of VRF routes to 1000. When the number of routes for the VRF reaches 1000, the router issues a syslog error message, but continues to accept new VRF routes.

```
Router(config)# ip vrf vrf1

Router(config-vrf)# rd 100:1

Router(config-vrf)# route-target import 100:1

Router(config-vrf)# maximum routes 1000 warning-only
```

The following example shows how to set the maximum number of VRF routes allowed to 1000 and set the warning threshold at 80 percent of the maximum. When the number of routes for the VRF reaches 800, the router issues a warning message. When the number of routes for the VRF reaches 1000, the router issues a SYSLOG error message and rejects any new routes.

```
Router(config)# ip vrf vrf2

Router(config-vrf)# rd 200:1

Router(config-vrf)# route-target import 200:1

Router(config-vrf)# maximum routes 1000 80
```

Related Commands

Command	Description
import map	Configures an import route map for a specified VRF for more control over routes imported into the VRF.
ip vrf	Specifies a name for a VPN routing and forwarding (VRF) routing table and enters VRF configuration mode.
rd	Creates VRF routing and forwarding tables and specifies the default route distinguisher for a VPN.
route-target	Configures a VRF route target community for importing and exporting extended community attributes.

metric-style narrow

To configure a router running Intermediate System-to-Intermediate System (IS-IS) so that it generates and accepts old-style type, length, and value objects (TLVs), use the **metric-style narrow** command in router configuration mode. To disable this function, use the **no** form of this command.

metric-style narrow [**transition**] [**level-1** | **level-2** | **level-1-2**]

no metric-style narrow [**transition**] [**level-1** | **level-2** | **level-1-2**]

Syntax Description

transition	(Optional) Instructs the router to use both old- and new-style TLVs.
level-1	(Optional) Enables this command on routing level 1.
level-2	(Optional) Enables this command on routing level 2.
level-1-2	(Optional) Enables this command on routing levels 1 and 2.

Defaults

The Multiprotocol Label Switching (MPLS) traffic engineering image generates only old-style TLVs. To do MPLS traffic engineering, a router must generate new-style TLVs that have wider metric fields.

Command Modes

Router configuration

Command History

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

Examples

The following example shows how to configure the router to generate and accept old-style TLVs on router level 1:

```
Router(config-router)# metric-style narrow level-1
```

Related Commands

Command	Description
metric-style transition	Configures a router to generate both old-style and new-style TLVs.
metric-style wide	Configures a router to generate and accept only new-style TLVs.

metric-style transition

To configure a router running Intermediate System-to-Intermediate System (IS-IS) so that it generates and accepts both old-style and new-style type, length, and value objects (TLVs), use the **metric-style transition** command in router configuration mode. To disable this function, use the **no** form of this command.

metric-style transition [**level-1** | **level-2** | **level-1-2**]

no metric-style transition [**level-1** | **level-2** | **level-1-2**]

Syntax Description		
	level-1	(Optional) Enables this command on routing level 1.
	level-2	(Optional) Enables this command on routing level 2.
	level-1-2	(Optional) Enables this command on routing levels 1 and 2.

Defaults The Multiprotocol Label Switching (MPLS) traffic engineering image generates only old-style TLVs. To do MPLS traffic engineering, a router must generate new-style TLVs that have wider metric fields.

Command Modes Router configuration

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

Examples The following example shows how to configure a router to generate and accept both old-style and new-style TLVs on router level 2:

```
Router(config-router)# metric-style transition level-2
```

Related Commands	Command	Description
	metric-style narrow	Configures a router to generate and accept old-style TLVs.
	metric-style wide	Configures a router to generate and accept only new-style TLVs.

metric-style wide

To configure a router running Intermediate System-to-Intermediate System (IS-IS) so that it generates and accepts only new-style type, length, and value objects (TLVs), use the **metric-style wide** command in router configuration mode. To disable this function, use the **no** form of this command.

metric-style wide [**transition**] [**level-1** | **level-2** | **level-1-2**]

no metric-style wide [**transition**] [**level-1** | **level-2** | **level-1-2**]

Syntax Description

transition	(Optional) Instructs the router to accept both old- and new-style TLVs.
level-1	(Optional) Enables this command on routing level 1.
level-2	(Optional) Enables this command on routing level 2.
level-1-2	(Optional) Enables this command on routing levels 1 and 2.

Defaults

The Multiprotocol Label Switching (MPLS) traffic engineering image generates only old-style TLVs. To do MPLS traffic engineering, a router must generate new-style TLVs that have wider metric fields.

Command Modes

Router configuration

Command History

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

Usage Guidelines

If you enter the **metric-style wide** command, a router generates and accepts only new-style TLVs. Therefore, the router uses less memory and other resources than it would if it generated both old-style and new-style TLVs.

This style is appropriate for enabling MPLS traffic engineering across an entire network.



Note

This discussion of metric styles and transition strategies is oriented toward traffic engineering deployment. Other commands and models could be appropriate if the new-style TLVs are desired for other reasons. For example, a network might require wider metrics, but might not use traffic engineering.

Examples

The following example shows how to configure a router to generate and accept only new-style TLVs on level 1:

```
Router(config-router)# metric-style wide level-1
```

Related Commands

Command	Description
metric-style narrow	Configures a router to generate and accept old-style TLVs.
metric-style transition	Configures a router to generate and accept both old-style and new-style TLVs.

mls rp ip

To enable the Multilayer Switching Protocol (MLSP) and Multilayer Switching (MLS), use the **mls rp ip** command in global configuration mode. To disable MLS, use the **no** form of this command.

mls rp ip

no mls rp ip

Syntax Description This command has no arguments or keywords.

Defaults Multilayer Switching (MLS) is disabled.

Command Modes Global configuration

Command History	Release	Modification
	11.3(3) WA4(4)	This command was introduced.

Usage Guidelines Use this command to enable MLS, either globally or on a specific interface. MLSP is the protocol that runs between the switches and routers.

Examples The following example enables MLS:

```
Router(config)# mls rp ip
```

Related Commands	Command	Description
	mls rp management-interface	Designates an interface as the management interface for MLSP packets.
	mls rp nde-address	Specifies a NetFlow Data Export address.
	mls rp vlan-id	Assigns a VLAN ID.
	mls rp vtp-domain	Selects the router interface to be Layer 3 switched and then adds that interface to a VTP domain.
	show mls rp	Displays MLS details, including specifics for MLSP.
	show mls rp vtp-domain	Displays MLS interfaces for a specific VTP domain.

mls rp ip multicast

To enable IP multicast Multilayer Switching (MLS) (hardware switching) on an external or internal router in conjunction with Layer 3 switching hardware for the Catalyst 5000, use the **mls rp ip multicast** command in interface configuration mode. To disable IP multicast MLS on the interface or virtual LAN (VLAN), use the **no** form of this command.

mls rp ip multicast

no mls rp ip multicast

Syntax Description This command has no arguments or keywords.

Defaults IP multicast MLS is enabled.

Command Modes Interface configuration

Command History

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

Usage Guidelines

This command is available only on specific router platforms connected to a Catalyst 5000 switch. Use this command to reduce multicast load on the router. The switch performs the multicast packet replication and forwarding.

IP multicast MLS is enabled by default on an interface once IP multicast routing and PIM are enabled.

Examples

The following example shows how to disable IP multicast MLS:

```
Router(config)# interface fastethernet1/0.1
Router(config-if)# no mls rp ip multicast
```

Related Commands

Command	Description
mls rp ip multicast management-interface	Assigns a different interface (other than the default) to act as the management interface for MLSP.
show ip mroute	Displays the contents of the IP multicast routing table.
show mls rp interface	Displays hardware-switched multicast flow information about IP multicast MLS.

mls rp ip multicast management-interface

To assign a different interface (other than the default) to act as the management interface for Multilayer Switching (MLS), use the **mls rp ip multicast management-interface** command in interface configuration mode. To restore the default interface as the management interface, use the **no** form of this command.

mls rp ip multicast management-interface

no mls rp ip multicast management-interface

Syntax Description

This command has no arguments or keywords.

Defaults

When IP multicast MLS is enabled, the subinterface (or virtual LAN [VLAN] interface) that has the lowest VLAN ID and is active (in the “up” state) is automatically selected as the management interface.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

When you enable IP multicast MLS, the subinterface (or VLAN interface) that has the lowest VLAN ID and is active (in the “up” state) is automatically selected as the *management interface*. The one-hop protocol Multilayer Switching Protocol (MLSP) is used between a router and a switch to pass messages about hardware-switched flows. MLSP packets are sent and received on the management interface. Typically, the interface in VLAN 1 is chosen (if that interface exists). Only one management interface is allowed on a single trunk link.

In most cases, we recommend that the management interface be determined by default. However, you can optionally use this command to specify a different router interface or subinterface as the management interface. We recommend using a subinterface with minimal data traffic so that multicast MLSP packets can be sent and received more quickly.

If the user-configured management interface goes down, the router uses the default interface (the active interface with the lowest VLAN ID) until the user-configured interface comes up again.

Examples

The following example shows how to configure the Fast Ethernet interface as the management interface:

```
Router(config)# interface fastethernet1/0.1  
Router(config-if)# mls rp ip multicast management-interface
```

Related Commands

Command	Description
mls rp ip multicast	Enables IP multicast MLS (hardware switching) on an external or internal router in conjunction with Layer 3 switching hardware for the Catalyst 5000 switch.

mls rp ipx (global)

To enable the router as an IPX Multilayer Switching (MLS) Route Processor (RP), use the **mls rp ipx** command in global configuration mode. To disable IPX MLS on the router, use the **no** form of this command.

mls rp ipx

no mls rp ipx

Syntax Description This command has no arguments or keywords.

Defaults IPX MLS is disabled.

Command Modes Global configuration

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

Usage Guidelines Multilayer Switching Protocol (MLSP) is the protocol that runs between the MLS Switching Engine and the MLS RP.

Examples The following example enables IPX MLS on the MLS RP:

```
Router(config)# mls rp ipx
```

Related Commands	Command	Description
	mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flows.
	mls rp management-interface	Designates an interface as the management interface for MLSP packets.
	mls rp vlan-id	Assigns a VLAN identification number to an IPX MLS interface.
	mls rp vtp-domain	Assigns an MLS interface to a specific VTP domain on the MLS RP.
	show mls rp interface	Displays IPX MLS details for the RP, including specific information about the MLSP.
	show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.
	show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the RP.

mls rp ipx (interface)

To enable IPX Multilayer Switching (MLS) on a router interface, use the **mls rp ipx** command in interface configuration mode. To disable IPX MLS on a router interface, use the **no** form of this command.

mls rp ipx

no mls rp ipx

Syntax Description This command has no arguments or keywords.

Defaults IPX MLS is disabled.

Command Modes Interface configuration

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

Usage Guidelines Multilayer Switching Protocol (MLSP) is the protocol that runs between the MLS Switching Engine and the MLS RP.

Examples The following example shows how to enable IPX MLS on a router interface:

```
Router(config-if)# mls rp ipx
```

Related Commands	Command	Description
	mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flows.
	mls rp management-interface	Designates an interface as the management interface for MLSP packets.
	mls rp vlan-id	Assigns a VLAN identification number to an IPX MLS interface.
	mls rp vtp-domain	Assigns an MLS interface to a specific VTP domain on the MLS RP.
	show mls rp interface	Displays IPX MLS details for the RP, including specific information about the MLSP.
	show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.
	show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the RP.

mls rp locate ipx

To display information about all switches currently shortcutting for the specified IPX flows, use the **mls rp locate ipx** command in privileged EXEC mode.

```
mls rp locate ipx destination-network.destination-node [source-network]
```

Syntax Description

<i>destination-network.destination-node</i>	The destination network and destination node of IPX packet flows. The destination network consists of 1 to 8 hexadecimal numbers in the format xxxxxxxx. The destination node consists of 1 to 12 hexadecimal numbers in the format xxxx.xxxx.xxxx.
<i>source-network</i>	(Optional) The source network of the IPX flow. The source network consists of 1 to 8 hexadecimal numbers in the format yyyyyyyy.

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to display the switch that is shortcutting routed flows to the specified IPX flow:

```
Router# mls rp locate ipx 30.0000.1111.2222

locator response from switch id 0010.1400.601f
```

Related Commands

Command	Description
mls rp ipx (global)	Enables the router as an IPX MLS RP.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp vlan-id	Assigns a VLAN identification number to an IPX MLS interface.
mls rp vtp-domain	Assigns an MLS interface to a specific VTP domain on the MLS RP.
show mls rp interface	Displays IPX MLS details for the RP, including specific information about the MLSP.
show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.
show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the RP.

mls rp management-interface

To specify an interface as the management interface, use the **mls rp management-interface** command in interface configuration mode. To remove an interface as the management interface, use the **no** form of this command.

mls rp management-interface

no mls rp management-interface

Syntax Description This command has no keywords or arguments.

Defaults No interface is specified as the management interface.

Command Modes Interface configuration

Command History

Release	Modification
11.3(3) WA4(4)	This command was introduced.

Usage Guidelines

Multilayer Switching Protocol (MLSP) packets are sent and received through the management interface. Select only one IPX Multilayer Switching (MLS) interface connected to the switch. If you fail to select this interface, no connection between the MLS Route Processor (RP) and the MLS Switching Engine occurs, and any routing updates or changes to access lists are not reflected on the switch.

Examples

The following example shows how to select a management interface:

```
Router(config-if)# mls rp management-interface
```

Related Commands

Command	Description
mls rp ipx (global)	Enables the router as an IPX MLS RP.
mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flows.
mls rp vlan-id	Assigns a VLAN identification number to an IPX MLS interface.
mls rp vtp-domain	Assigns an MLS interface to a specific VTP domain on the MLS RP.
show mls rp interface	Displays IPX MLS details for the RP, including specific information about the MLSP.
show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.
show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the RP.

mls rp nde-address

To specify a NetFlow Data Export (NDE) address, use the **mls rp nde-address** command in global configuration mode.

mls rp nde-address *ip-address*

Syntax Description	<i>ip-address</i>	NDE IP address.
---------------------------	-------------------	-----------------

Defaults	No NDE address is specified.
-----------------	------------------------------

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

Command History	Release	Modification
	11.3(3) WA4(4)	This command was introduced.

Usage Guidelines	Use this command on a Route Processor (RP) to specify the NDE address for a router. If you <i>do not</i> specify an NDE IP address for the Multilayer Switching (MLS) RP, the MLS RP automatically selects one of its interface's IP addresses and uses that IP address as its NDE IP address <i>and</i> its MLS IP address.
-------------------------	--

Examples	The following example shows how to set the NDE address to 172.25.2.1:
-----------------	---

```
Router(config)# mls rp nde-address 172.25.2.1
```

Related Commands	Command	Description
	mls rp ip	Enables MLSP.
	mls rp management-interface	Designates an interface as the management interface for MLSP packets.
	mls rp vlan-id	Assigns a VLAN ID.
	mls rp vtp-domain	Selects the router interface to be Layer 3 switched and then adds that interface to a VTP domain.
	show mls rp	Displays MLS details, including specifics for MLSP.
	show mls rp vtp-domain	Displays MLS interfaces for a specific VTP domain.

mls rp vlan-id

To assign a virtual LAN (VLAN) identification number to an IPX Multilayer Switching (MLS) interface, use the **mls rp vlan-id** command in interface configuration mode. To remove a VLAN identification number, use the **no** form of this command.

mls rp vlan-id *vlan-id-number*

no mls rp vlan-id *vlan-id-number*

Syntax Description

vlan-id-number A VLAN identification number from 1 to 4096.

Defaults

No VLAN identification number is assigned.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(3) WA4(4)	This command was introduced.

Usage Guidelines

The assigned IPX MLS interface must be either an Ethernet or Fast Ethernet interface—both without subinterfaces.

Examples

The following example shows how to assign the VLAN identification number 23 to an IPX MLS interface:

```
Router(config-if)# mls rp vlan-id 23
```

Related Commands

Command	Description
mls rp ipx (global)	Enables the router as an IPX MLS RP.
mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flows.
mls rp management-interface	Designates an interface as the management interface for MLSP packets.
mls rp vtp-domain	Assigns an MLS interface to a specific VTP domain on the MLS RP.
show mls rp interface	Displays IPX MLS details for the RP, including specific information about the MLSP.
show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.
show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the RP.

mls rp vtp-domain

To assign a Multilayer Switching (MLS) interface to a specific Virtual Trunk Protocol (VTP) domain on the MLS Route Processor (RP), use the **mls rp vtp-domain** command in interface configuration mode. To remove a VTP domain, use the **no** form of this command.

mls rp vtp-domain *domain-name*

no mls rp vtp-domain *domain-name*

Syntax Description	<i>domain-name</i>	The name of the VTP domain assigned to an MLS interface and its related switches.
---------------------------	--------------------	---

Defaults	The interface is assigned to the null domain.
-----------------	---

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

Command History	Release	Modification
	11.3(3) WA4(4)	This command was introduced.

Usage Guidelines	The assigned IPX MLS interface must be either an Ethernet or Fast Ethernet interface—both without subinterfaces.
-------------------------	--

Examples	The following example shows how to assign the MLS interface to the VTP domain named engineering: Router(config-if)# mls rp vtp-domain engineering
-----------------	---

Related Commands	Command	Description
	mls rp ipx (global)	Enables the router as an IPX MLS RP.
	mls rp locate ipx	Displays information about all switches currently shortcutting for the specified IPX flows.
	mls rp management-interface	Designates an interface as the management interface for MLSP packets.
	mls rp vlan-id	Assigns a VLAN identification number to an IPX MLS interface.
	show mls rp interface	Displays IPX MLS details for the RP, including specific information about the MLSP.
	show mls rp ipx	Displays details for all IPX MLS interfaces on the IPX MLS router.
show mls rp vtp-domain	Displays IPX MLS interfaces for a specific VTP domain on the RP.	

monitor session

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

To start a new Switched Port Analyzer (SPAN) session, add or delete interfaces from an existing SPAN session, or delete a SPAN session, use the **monitor session** command in global configuration mode. To remove one or more source interfaces or destination interfaces from the SPAN session, use the **no** form of this command.

Source Interface

```
monitor session session {source {interface type/slot/port} [, | - | rx | tx | both]
no monitor session session {source {interface type/slot/port} [, | - | rx | tx | both]}
```

Destination Interface

```
monitor session session {destination {interface type/slot/port} [, | -]}
no monitor session session {destination {interface type/slot/port} [, | -]}
```

Session

```
monitor session session
no monitor session session
```

Catalyst Switches

To start a new SPAN session, add or delete interfaces or VLANs to or from an existing SPAN session, filter SPAN traffic to specific VLANs, or delete a SPAN session, use the **monitor session** command in global configuration mode. To remove one or more source or destination interfaces from the SPAN session or a source VLAN from the SPAN session, use the **no** form of this command.

Source Interface or VLAN

```
monitor session session {source {interface type number} | {vlan vlan-id} [, | - | rx | tx | both]
no monitor session session {source {interface type number} | {vlan vlan-id} [, | - | rx | tx | both]}
```

Destination Interface or VLAN

```
monitor session session {destination {interface type number} [, | -] | {vlan vlan-id}}
no monitor session session {destination {interface type number} [, | -] | {vlan vlan-id}}
```

Filter VLAN

```
monitor session session {filter {vlan vlan-id} [, | -]}
no monitor session session {filter {vlan vlan-id} [, | -]}
```

Syntax Description

<i>session</i>	Number of the SPAN session; valid values are 1 and 2 .
source	Specifies the SPAN source.

destination	Specifies the SPAN destination interface.
interface type	(Optional) Specifies the interface type; valid values are fastethernet and gigabitethernet .
<i>slot</i>	(Optional) Specifies interface number; valid entries are 1 or 2 .
<i>port</i>	(Optional) Port interface number ranges based on type of Ethernet switch network module used: 0 to 15 for NM-16ESW 0 to 35 for NM-36ESW 0 to 1 for GigabitEthernet
interface type number	Specifies the interface type and number; valid values are ethernet (1 to 9), fastethernet (1 to 9), gigabitethernet (1 to 9), and port-channel (see the “Usage Guidelines” section).
filter	Limits SPAN source traffic to specific VLANs. Note The filter keyword is not supported on the Cisco 2600 series or the Cisco 3600 series routers.
vlan vlan-id	Specifies the VLAN; valid values are from 1 to 1005.
,	(Optional) Specifies another range of SPAN VLANs; valid values are from 1 to 1005.
-	(Optional) Specifies a range of SPAN VLANs.
rx	(Optional) Specifies monitor received traffic only.
tx	(Optional) Specifies monitor transmitted traffic only.
both	(Optional) Specifies monitor received and transmitted traffic.

Defaults

A trunking interface monitors all VLANs and all received and transmitted traffic.

Command Modes

Global 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.
12.1(3a)E3	The number of valid values for the port-channel number was changed; see the “Usage Guidelines” section for valid values.
12.1(5c)EX	These SPAN support restrictions were added: <ul style="list-style-type: none"> • If your switch has a Switch Fabric Module installed, SPAN is supported among supervisor engines and nonfabric-enabled modules. • If your switch does not have a Switch Fabric Module installed, SPAN is supported on all modules, including fabric-enabled modules. • SPAN on DFC-equipped modules is not supported.

Release	Modification
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**Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers**

The **port-channel** number supports six EtherChannels and eight ports in each channel.

Only one SPAN destination for a SPAN session is supported. If you attempt to add another destination interface to a session that already has a destination interface configured, you will get an error. You must first remove a SPAN destination interface before changing the SPAN destination to a different interface.

Catalyst Switches

The number of valid values for **port-channel** number depends on the software release. For Cisco IOS releases prior to software Release 12.1(3a)E3, valid values are from 1 to 256; for Cisco IOS Release 12.1(3a)E3, 12.1(3a)E4, and 12.1(4)E1, valid values are from 1 to 64. Cisco IOS Release 12.1(5c)EX and later support a maximum of 64 values ranging from 1 to 256.

Only one destination per SPAN session is supported. If you attempt to add another destination interface to a session that already has a destination interface configured, you get an error. You must first remove a SPAN destination interface before changing the SPAN destination to a different interface.

You can configure up to 64 SPAN destination interfaces, but you can have one egress SPAN source interface and up to 64 ingress source interfaces only.

A SPAN session can either monitor VLANs or monitor individual interfaces, but it cannot monitor both specific interfaces and specific VLANs. Configuring a SPAN session with a source interface and then trying to add a source VLAN to the same SPAN session causes an error. Configuring a SPAN session with a source VLAN and then trying to add a source interface to that session also causes an error. You must first clear any sources for a SPAN session before switching to another type of source.

If you enter the **filter** keyword on a monitored trunk interface, only traffic on the set of specified VLANs is monitored.

Port channel interfaces display in the list of **interface** options if you have them configured. VLAN interfaces are not supported. However, you can span a particular VLAN by entering the **monitor session session source vlan vlan-id** command.

Examples**Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers**

The following example shows how to add a destination VLAN to an existing SPAN session:

```
Router(config)# monitor session 1 destination interface fastEthernet 2/0
```

Catalyst Switches

The following example shows how to add a destination VLAN to an existing SPAN session:

```
Router(config)# monitor session 1 destination vlan 100
```

The following example shows how to delete a destination VLAN from an existing SPAN session:

```
Router(config)# no monitor session 1 destination vlan 100
```

The following example shows how to limit SPAN traffic to specific VLANs:

```
Router(config)# monitor session 1 filter vlan 100 - 304
```

Related Commands

Command	Description
show monitor	Displays SPAN session information.

mpls atm control-vc

To configure the control-VC virtual path identifier (VPI) and virtual circuit identifier (VCI) values for the initial link to the Multiprotocol Label Switching (MPLS) peer, use the **mpls atm control-vc** command in interface configuration mode. To unconfigure the values, use the **no** form of this command.

mpls atm control-vc *vpi vci*

no mpls atm control-vc *vpi vci*

Syntax Description

<i>vpi</i>	Virtual path identifier, in the range from 0 to 4095.
<i>vci</i>	Virtual circuit identifier, in the range from 0 to 65535.

Defaults

0/32

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(4)T	This command was updated to reflect the MPLS IETF terminology. The VPI range of values was extended to 4095.

Usage Guidelines

Use this command to establish the LDP session and to carry non-IP traffic. The default VPI VCI for the control VC is (3, 32). If for any reason you need to have a different control-VC, use the **mpls atm control-vc** command to configure any VPI VCI allowed by the *vpi* and *vci* arguments for the control VC.

Examples

The following example shows how to create an MPLS subinterface on a router and select VPI 1 and VCI 34 as the control VC:

```
Router(config)# interface atm4/0.1 mpls
Router(config-if)# mpls ip
Router(config-if)# mpls atm control-vc 1 34
```

Related Commands

Command	Description
mpls ip (interface)	Enables label switching of IPv4 packets on an interface.

mpls atm cos

To change the configured bandwidth allocation for class of service (CoS), use the **mpls atm cos** command in global configuration mode.

mpls atm cos { **available** | **standard** | **premium** | **control** } *weight*

Syntax Description		
	available	The weight for the available class. This is the lowest class priority.
	standard	The weight for the standard class. This is the next lowest class priority.
	premium	The weight for the premium class. This is the next highest class priority.
	control	The weight for the control class. This is the highest class priority.
	<i>weight</i>	The total weight for all CoS traffic classes. This value ranges from 0 to 100.

Defaults Available 50%, control 50%

Command Modes Global configuration

Command History	Release	Modifications
	12.0(5)T	This command was introduced.
	12.2(4)T	This command was updated to reflect the MPLS IETF terminology.

Examples The following example shows how to configure the XTagATM interface for CoS traffic:

```
Router(config)# interface xtagatm12
Router(config-if)# extended-port atm1/0 descriptor 1.2
Router(config-if)# mpls ip
Router(config-if)# mpls atm cos available 49
Router(config-if)# mpls atm cos standard 50
Router(config-if)# mpls atm cos premium 0
Router(config-if)# mpls atm cos control 1
```

mpls atm disable-headend-vc

To remove all headend virtual circuits (VCs) from the Multiprotocol Label Switching (MPLS) Label Switch Controller (LSC) and disable its ability to function as an edge label switch router (LSR), use the **mpls atm disable-headend-vc** command in global configuration mode. To restore the headend VCs of the MPLS LSC and restores full edge LSR functionality, use the **no** form of this command.

mpls atm disable-headend-vc

no mpls atm disable-headend-vc

Syntax Description This command has no arguments or keywords.

Defaults Edge LSR Enabled

Command Modes Global configuration

Command History	Release	Modification
	12.0(7)DC	This command was introduced.
	12.2(4)T	This command was updated to reflect the MPLS IETF terminology.

Usage Guidelines This command prevents the LSC from initiating headend label VCs (LVCs), and thus reduces the number of LVCs used in the network.

Examples The following example shows how to disable the MPLS LSC from acting like an edge LSR and therefore cannot create headend LVCs:

```
mpls atm disable-headend-vc
```

mpls atm multi-vc

To configure a router subinterface to create one or more label virtual circuits (VCs) over which packets of different classes are sent, use the **mpls atm multi-vc** command in ATM subinterface submode. To remove the label virtual circuits, use the **no** form of this command.

mpls atm multi-vc

no mpls atm multi-vc

Syntax Description This command has no arguments or keywords.

Command Modes ATM subinterface submode

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.0(10)ST	This command was modified to reflect Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) syntax and terminology.
	12.2(2)T	This command was integrated into the Cisco IOS Release 12.2(2)T.

Usage Guidelines This command is valid only on ATM MPLS subinterfaces.

Examples The following example shows how to configure interface ATM2/0/0.1 on the networking device for MPLS quality of service (QoS) multi-VC mode:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface ATM2/0/0.1 mpls
Router(config-subif)# mpls atm multi-vc
Router(config-subif)# exit
Router(config)# exit
```

Related Commands	Command	Description
	mpls cos-map	Creates a class map that specifies how classes map to label virtual circuits when they are combined with a prefix map.
	mpls prefix-map	Configures a networking device to use a specified QoS map when a label destination prefix matches the specified access list.

mpls atm vpi

To configure the range of values to use in the virtual path identifier (VPI) field for label virtual circuits (LVCs), use the **mpls atm vpi** command in interface configuration mode. To clear the range of values, use the **no** form of this command.

```
mpls atm vpi vpi [- vpi] [vci-range low - high]
```

```
no mpls atm vpi vpi [- vpi] [vci-range low - high]
```

Syntax Description

<i>vpi</i>	Virtual path identifier, low end of range (0 to 4095).
- <i>vpi</i>	(Optional) Virtual path identifier, high end of range (0 to 4095).
vci-range <i>low - high</i>	(Optional) Range of virtual channel identifier (VCI) values the subinterface can use for the VPI(s).

Defaults

The default VPI range is 1-1.

The default VCI range is 33-65535.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(4)T	This command was updated to reflect the MPLS IETF terminology. The vci-range keyword was added. The VPI range of values was extended to 4095.

Usage Guidelines

You might need to change the default tag virtual path identifier (VPI) range on the switch if:

- It is an administrative policy to use a VPI value other than 1, the default VPI.
- There are many LVCs on an interface.

To configure ATM MPLS on a router interface (for example, an ATM Interface Processor), you must enable an MPLS subinterface.



Note

The **mpls atm control-vc** and **mpls atm vpi** subinterface level configuration commands are available on any interface that can support ATM labeling.

Use this command to select an alternate range of VPI values for ATM label assignment on this interface. The two ends of the link negotiate a range defined by the intersection of the range configured at each end.

- To configure the VPI range for an edge label switch router (edge LSR) subinterface connected to another router or to an LSC, limit the range to four VPIs.
- For an ATM-LSR, the VPI range specified must lie within the range that was configured on the ATM switch for the corresponding ATM switch interface.
- If the LDP neighbor is a router, the VPI range can be no larger than two. For example, you can specify from 5 to 6 (a range of two), not 5 to 7 (a range of three). If the LDP neighbor is a switch, the maximum VPI range is 0 to 255.

If you use the **vci-range** keyword, you must specify a VPI value.

Examples

The following example shows how to create a subinterface and selects a VPI range from VPI 1 to VPI 3:

```
Router(config)# interface atm4/0.1 mpls
Router(config-if)# mpls ip
Router(config-if)# mpls atm vpi 1-3
```

The following example shows how to create a subinterface with a VPI of 240 and a VCI range between 33 and 4090:

```
Router(config)# interface atm4/0.1 mpls
Router(config-if)# mpls ip
Router(config-if)# mpls atm vpi 240 vci-range 33-4090
```

Related Commands

Command	Description
mpls atm control-vc	Configures VPI and VCI values for the initial link to an MPLS peer.

mpls atm vp-tunnel

To specify an interface or a subinterface as a virtual path (VP) tunnel, use the **mpls atm vp-tunnel** command in interface configuration mode. To remove the VP tunnel from an interface or subinterface, use the **no** form of this command.

mpls atm vp-tunnel *vpi* [**vci-range** *low - high*]

no mpls atm vp-tunnel *vpi* [**vci-range** *low - high*]

Syntax Description

<i>vpi</i>	Virtual path identifier (VPI) value for the local end of the tunnel (0 to 4095).
vci-range <i>low - high</i>	(Optional) Range of virtual channel identifier (VCI) values the VP tunnel can use.

Defaults

If you do not specify a VCI range for the VP tunnel, the tunnel uses the default VCI range of 33-65535.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(4)T	This command was updated to reflect the Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) terminology. The vci-range keyword was added. The VPI range of values was extended to 4095.

Usage Guidelines

The **mpls atm vp-tunnel** and **mpls atm vpi** commands are mutually exclusive.

This command is available on both extended MPLS ATM (XTagATM) interfaces and on LC-ATM subinterfaces of router ATM interfaces. The command is not available on the LS1010, where all subinterfaces are automatically VP tunnels.

It is not necessary to use the **mpls atm vp-tunnel** command on an XTagATM interface in most applications. The switch learns (through VSI interface discovery) whether the XTagATM interface is a tunnel, the VPI value of the tunnel, and tunnel status.

Examples

The following example shows how to create an MPLS subinterface VP tunnel with a VPI value of 4:

```
Router(config-if)# mpls atm vp-tunnel 4
```

The following example shows how to create a VP tunnel with a value of 240 and a VCI range of 33 to 4090:

```
Router(config-if)# mpls atm vp-tunnel 240 vci-range 33-4090
```

mpls cos-map

To create a class map that specifies how classes map to label virtual circuits (VCs) when they are combined with a prefix map, use the **mpls cos-map** command in global configuration mode.

mpls cos-map *cos-map*

Syntax Description

<i>cos-map</i>	Number from 1 to 155 that identifies the class map.
----------------	---

Defaults

No class maps are specified.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(10)ST	This command was modified to reflect Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) syntax and terminology.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Examples

The following example shows how to create a class map:

```
Router(config)# mpls cos-map 55
Router(config-mpls-cos-map)# class 1 premium
Router(config-mpls-cos-map)# exit
Router(config)#
```

Related Commands

Command	Description
show mpls cos-map	Displays the QoS map used to assign a quantity of label virtual circuits and the associated class of service for those label virtual circuits.

mpls ip (global configuration)

To enable Multiprotocol Label Switching (MPLS) forwarding of IP version 4 (IPv4) packets along normally routed paths for the platform, use the **mpls ip** command in global configuration mode. To disable MPLS forwarding of IPv4 packets, use the **no** form of this command.

mpls ip

no mpls ip

Syntax Description This command has no arguments or keywords.

Defaults MPLS forwarding of IPv4 packets along normally routed paths is enabled for the platform.

Command Modes Global configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines

MPLS forwarding of IPv4 packets along normally routed paths (sometimes called dynamic label switching) is enabled by this command. Enabling MPLS forwarding of IP packets for the platform does not enable it for a platform interface. For a given interface to perform dynamic label switching, this switching function must be enabled for the interface as well as for the platform.



Note

Globally enabling MPLS forwarding of IPv4 packets for the platform is not sufficient by itself to initiate label distribution. The Label Distribution Protocol (LDP)/Tag Distribution Protocol (TDP) is not initialized until you configure MPLS forwarding of IPv4 packets for some interface or you configure a targeted session. See the [“mpls ip \(interface configuration\)”](#) section.

The **no** form of this command stops dynamic label switching for all platform interfaces, regardless of the interface configuration; it also stops distribution of labels for dynamic label switching. Instead of entering the **no mpls ip** command individually for each interface, you can stop dynamic label switching on all platform interfaces by entering the command once in global configuration mode. You can then reenabling label switching for all platform interfaces by entering an **mpls ip** command in global configuration mode. (This is commonly known as globally toggling MPLS IP [**no mpls ip/mpls ip**].)

For a label-controlled ATM (LC-ATM) interface, the **no** form of this command prevents the establishment of label virtual circuits originating at, terminating at, or passing through the platform.

The **no mpls ip** command does not affect the sending of labeled packets through label switch path (LSP) tunnels.

Examples

The following example shows how to disable dynamic label switching for the platform and how to terminate all label distribution for the platform:

```
Router(config)# no mpls ip
```

Related Commands

Command	Description
mpls ip (interface configuration)	Enables MPLS forwarding of IPv4 packets along normally routed paths for a particular interface

mpls ip (interface configuration)

To enable Multiprotocol Label Switching (MPLS) forwarding of IP version 4 (IPv4) packets along normally routed paths for a particular interface, use the **mpls ip** command in interface configuration mode. To disable MPLS forwarding of IPv4 packets, use the **no** form of the command.

mpls ip

no mpls ip

Syntax Description This command has no arguments or keywords.

Defaults MPLS forwarding of IPv4 packets along normally routed paths is disabled for the interface.

Command Modes Interface configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines

MPLS forwarding of IPv4 packets along normally routed paths is sometimes called dynamic label switching. If dynamic label switching is enabled for the platform when this command is issued on an interface, label distribution for the interface begins with the periodic transmission of neighbor Discovery Hello messages on the interface. The **mpls ip (interface configuration)** command works in conjunction with the **mpls ip (global configuration)** command to enable label distribution for the platform interface. When the outgoing label for a destination that is routed through the interface is known, packets for the destination are assigned that outgoing label and forwarded through the interface.



Note

Enabling MPLS forwarding of IPv4 packets for an interface is not sufficient by itself to initiate label distribution. MPLS forwarding of IPv4 packets must also be enabled for the platform before label distribution begins (see the “[mpls ip \(global configuration\)](#)” section).

The **no** form of this command causes packets routed out through the interface to be sent unlabeled; this form of the command also terminates label distribution for the interface. However, the **no** form of the command does not affect the sending of labeled packets through any LSP tunnels that might use the interface.

For a label-controlled ATM (LC-ATM) interface, the **no** form of this command prevents the establishment of label virtual circuits beginning at, terminating at, or passing through the interface.

Examples

The following example shows how to enable label switching on the specified Ethernet interface:

```
Router(config)# configure terminal
Router(config-if)# interface Ethernet 0/2
Router(config-if)# mpls ip
```

Related Commands

Command	Description
mpls ip (global configuration)	Enables label switching of IPv4 packets along normally routed paths for the platform.
mpls ldp maxhops	Limits the number of hops permitted in an LSP established by the Downstream-on-Demand method of label distribution.
show mpls interfaces	Displays information about one or more interfaces that have been configured for label switching.

mpls ip default-route

To enable the distribution of labels associated with the IP default route, use the **mpls ip default-route** command in global configuration mode.

mpls ip default-route

Syntax Description This command has no arguments or keywords.

Defaults No distribution of labels for the IP default route.

Command Modes Global configuration

Command History	Release	Modification
	11.1 CT	This command was introduced.
	12.1(3)T	This command was modified to reflect new Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) terminology.

Usage Guidelines Dynamic label switching (that is, distribution of labels based on routing protocols) must be enabled before you can use the **mpls ip default-route** command.

Examples The following example shows how to enable the distribution of labels associated with the IP default route:

```
Router# configure terminal
Router(config)# mpls ip
Router(config)# mpls ip default-route
```

Related Commands	Command	Description
	mpls ip (global configuration)	Enables MPLS forwarding of IPv4 packets along normally routed paths for the platform.
	mpls ip (interface configuration)	Enables MPLS forwarding of IPv4 packets along normally routed paths for a particular interface.

mpls ip encapsulate explicit-null

To encapsulate all packets forwarded from the interface or subinterface with an explicit NULL label header, use the **mpls ip encapsulate explicit-null** command in interface configuration or subinterface configuration mode. To disable this function, use the **no** form of this command.

mpls ip encapsulate explicit-null

no mpls ip encapsulate explicit-null

Syntax Description

This command has no arguments or keywords.

Defaults

Packets are sent out without an explicit NULL label header.

Command Modes

Interface configuration
Subinterface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This is a per-interface command. The command establishes an explicit NULL LSP at the customer edge (CE) router. If MPLS is configured on a router and you enter this command, an error message occurs. This command is also supported on the Cisco 2600 series and Cisco 3600 series platforms.

Examples

The following example shows how to encapsulate all packets forwarded onto the interface or subinterface with an explicit NULL label header:

```
Router(config-if)# mpls ip encapsulate explicit-null
```