

show tag-switching tdp discovery

The **show tag-switching tdp discovery** command is replaced by the **show mpls ldp discovery** command. See the [show mpls ldp discovery](#) command for more information.

show tag-switching tdp neighbors

The **show tag-switching tdp neighbors** command is replaced by the **show mpls ldp neighbors** command. See the [show mpls ldp neighbor](#) command for more information.

show tag-switching tdp parameters

The `show tag-switching tdp parameters` command is replaced by the `show mpls ldp parameters` command. See the [show mpls ldp parameters](#) command for more information.

show vlans

To view virtual LAN (VLAN) subinterfaces, use the **show vlans** command in privileged EXEC mode.

show vlans

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.0	This command was introduced.
	12.1(3)T	This command was modified to display traffic count on FastEthernet subinterfaces.

Examples The following is sample output from the **show vlans** command:

```
Router# show vlans

Virtual LAN ID: 2 (IEEE 802.1Q Encapsulation)

    vLAN Trunk Interface:  FastEthernet5/0.1

    Protocols Configured:  Address:          Received:      Transmitted:
                          IP              56.0.0.3      16            92129

Virtual LAN ID: 3 (IEEE 802.1Q Encapsulation)

    vLAN Trunk Interface:  Ethernet6/0/1.1

    Protocols Configured:  Address:          Received:      Transmitted:
                          IP              36.0.0.3      1558          1521

Virtual LAN ID: 4 (Inter Switch Link Encapsulation)

    vLAN Trunk Interface:  FastEthernet5/0.2

    Protocols Configured:  Address:          Received:      Transmitted:
                          IP              76.0.0.3      0             7
```

The following is sample output from the **show vlans** command indicating a native VLAN and a bridged group:

```
Virtual LAN ID: 1 (IEEE 802.1Q Encapsulation)

    vLAN Trunk Interface:  FastEthernet1/0/2

    This is configured as native Vlan for the following interface(s) :

FastEthernet1/0/2

    Protocols Configured:  Address: Received:      Transmitted:
```

```

Virtual LAN ID: 100 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interface: FastEthernet1/0/2.1

Protocols Configured: Address: Received: Transmitted:

    Bridging      Bridge Group 1 0          0

```

Table 117 describes the significant fields shown in the display.

Table 117 *show vlans Field Descriptions*

Field	Description
Virtual LAN ID	Domain number of the VLAN.
vLAN Trunk Interface	Subinterface that carries the VLAN traffic.
Protocols Configured	Protocols configured on the VLAN.
Address	Network address.
Received	Packets received.
Transmitted	Packets sent.

show vlan-switch

To display virtual LAN (VLAN) information, use the **show vlan-switch** command in privileged EXEC mode.

```
show vlan-switch [brief | id vlan | name name]
```

Syntax Description	Parameter	Description
	brief	(Optional) Displays only a single line for each VLAN, naming the VLAN, status, and ports.
	id <i>vlan</i>	(Optional) Displays information about a single VLAN identified by VLAN ID number; valid values are from 1 to 1005.
	name <i>name</i>	(Optional) Displays information about a single VLAN identified by VLAN name; valid values are an ASCII string from 1 to 32 characters.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(2)XT	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

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

Examples The following example shows how to display the VLAN parameters for all VLANs within the administrative domain:

```
Router# show vlan-switch
```

```

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

```

```


1004 fddinet-default          active
1005 trnet-default           active

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

```

Table 118 describes the significant fields shown in the display.

Table 118 show vlan Field Descriptions

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

show vtp

To display general information about the virtual LAN (VLAN) Trunk Protocol (VTP) management domain, status, and counters, use the **show vtp** command in privileged EXEC mode.

```
show vtp {counters | status}
```

Syntax Description

counters	Displays the VTP counters for the switch.
status	Displays the general information about the VTP management domain.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2(8)SA4	This command was introduced.
12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Examples

The following is sample output from the **show vtp counters** command:

```
Router# show vtp counters
```

```
VTP statistics:
```

```
Summary advertisements received    : 38
Subset advertisements received     : 0
Request advertisements received    : 0
Summary advertisements transmitted : 13
Subset advertisements transmitted  : 3
Request advertisements transmitted : 0
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0
```

```
VTP pruning statistics:
```

```
Trunk          Join Transmitted Join Received    Summary advts received from
                |                |                | non-pruning-capable device
-----|-----|-----|-----
Fa0/9          827                824                0
Fa0/10         827                823                0
Fa0/11         827                823                0
```

Table 119 describes the significant fields shown in the display.

Table 119 *show vtp counters Field Descriptions*

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

Table 119 *show vtp counters Field Descriptions (continued)*

Field	Description
Number of config digest errors	<p>Number of MD5 digest errors.</p> <p>Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the switch do not match. This error usually indicates that the VTP password in the two switches is different. To solve this problem, make sure the VTP password on all switches is the same.</p> <p>These errors indicate that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.</p>
Number of V1 summary errors	<p>Number of version 1 errors.</p> <p>Version 1 summary errors increment whenever a switch in VTP V2 mode receives a VTP version 1 frame. These errors indicate that at least one neighboring switch is either running VTP version 1 or VTP version 2 with V2-mode disabled. To solve this problem, change the configuration of the switches in VTP V2-mode to disabled.</p>
Join Transmitted	Number of VTP pruning messages transmitted on the trunk.
Join Received	Number of VTP pruning messages received on the trunk.
Summary Advts Received from non-pruning-capable device	Number of VTP summary messages received on the trunk from devices that do not support pruning.

The following is sample output from the **show vtp status** command:

```
Router# show vtp status

VTP Version                : 2
Configuration Revision     : 1
Maximum VLANs supported locally : 68
Number of existing VLANs   : 7
VTP Operating Mode        : Server
VTP Domain Name           : test1
VTP Pruning Mode          : Disabled
VTP V2 Mode               : Disabled
VTP Traps Generation      : Disabled
MD5 digest                 : 0x3D 0x02 0xD4 0x3A 0xC4 0x46 0xA1 0x03
Configuration last modified by 172.20.130.52 at 3-4-93 22:25:
```

Table 120 describes the significant fields shown in the display.

Table 120 *show vtp status Field Descriptions*

Field	Description
VTP Version	<p>Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers</p> <p>Displays the VTP version operating on the switch. By default, switches implement version 1.</p> <p>Catalyst Switches</p> <p>Displays the VTP version operating on the switch. By default, Catalyst 2900 and 3500 XL switches implement version 1 but can be set to version 2.</p>
Configuration Revision	Current configuration revision number on this switch.
Maximum VLANs Supported Locally	Maximum number of VLANs supported locally.
Number of Existing VLANs	Number of existing VLANs.

Table 120 show vtp status Field Descriptions (continued)

Field	Description
VTP Operating Mode	<p data-bbox="808 317 1515 373">Displays the VTP operating mode, which can be server, client, or transparent.</p> <p data-bbox="808 394 1515 548">Server—A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch guarantees that it can recover all VLAN information in the current VTP database from nonvolatile storage after reboot. By default, every switch is a VTP server.</p> <p data-bbox="808 569 1515 751">Client—A switch in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not transmit VTP advertisements until it receives advertisements to initialize its VLAN database.</p> <p data-bbox="808 772 1515 1018">Transparent—A switch in VTP transparent mode is disabled for VTP, does not transmit advertisements or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received. The configuration of multi-VLAN ports causes the switch to automatically enter transparent mode.</p> <p data-bbox="808 1039 1515 1285">Note Catalyst 2912MF, 2924M, and 3500 XL switches support up to 250 VLANs. All other Catalyst 2900 XL switches support up to 64 VLANs. If you define more than 250 or 64 or if the switch receives an advertisement that contains more than 250 or 64 VLANs, the switch automatically enters VTP transparent mode and operates with the VLAN configuration preceding the one that sent it into transparent mode.</p> <p data-bbox="808 1318 1515 1409">Note Catalyst 2912MF, 2924M, and 3500 XL switches support up to 250 VLANs. All other Catalyst 2900 XL switches support up to 64 VLANs.</p> <p data-bbox="889 1444 1515 1627">For Catalyst 2912MF, 2924M, and 3500 XL switches, if you define more than 250 or if the switch receives an advertisement that contains more than 250 VLANs, the switch automatically enters VTP transparent mode and operates with the VLAN configuration preceding the one that sent it into transparent mode.</p> <p data-bbox="889 1669 1515 1852">For all other Catalyst 2900 XL switches, if you define more than 64 or if the switch receives an advertisement that contains more than 64 VLANs, the switch automatically enters VTP transparent mode and operates with the VLAN configuration preceding the one that sent it into transparent mode.</p>
VTP Domain Name	Name that identifies the administrative domain for the switch.

Table 120 show vtp status Field Descriptions (continued)

Field	Description
VTP Pruning Mode	<p>Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers</p> <p>VTP pruning mode is not supported on the Cisco 2600 series and Cisco 3600 series routers.</p> <p>Catalyst Switches</p> <p>Displays whether pruning is enabled or disabled. Enabling pruning on a VTP server enables pruning for the entire management domain. Pruning restricts flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.</p>
VTP V2 Mode	Displays if VTP version 2 mode is enabled. All VTP version 2 switches operate in version 1 mode by default. Each VTP switch automatically detects the capabilities of all other VTP devices. A network of VTP devices should be configured to version 2 only if all VTP switches in the network can operate in version 2 mode.
VTP Traps Generation	Displays whether VTP traps are transmitted to a network management station.
MD5 Digest	16-byte checksum of the VTP configuration.
Configuration Last Modified	Displays the date and time of the last configuration modification. Displays the IP address of the switch that caused the configuration change to the database.

Related Commands

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

show xtagatm cos-bandwidth-allocation xtagatm

To display information about quality of service (QoS) bandwidth allocation on extended Multiprotocol Label Switching (MPLS) ATM (XTagATM) interfaces, use the **show xtagatm cos-bandwidth-allocation xtagatm** command in user EXEC or privileged EXEC mode.

```
show xtagatm cos-bandwidth-allocation xtagatm [xtagatm interface number]
```

Syntax Description

xtagatm *interface number* (Optional) Specifies the XTagATM interface number.

Defaults

Available 50 percent, control 50 percent.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

Use this command to display QoS bandwidth allocation information for the following QoS traffic categories:

- Available
- Standard
- Premium
- Control

Examples

The following example shows output from this command:

```
Router# show xtagatm cos-bandwidth-allocation xtagatm 123

CoS           Bandwidth allocation
available     25%
standard      25%
premium       25%
control       25%
```

show xtagatm cross-connect

To display information about the Label Switch Controller (LSC) view of the cross-connect table on the remotely controlled ATM switch, use the **show xtagatm cross-connect** command in user EXEC or privileged EXEC mode.

```
show xtagatm cross-connect [traffic] [interface interface [vpi vci] | descriptor descriptor
                             [vpi vci]]
```

Syntax Description		
<i>traffic</i>	(Optional)	Displays receive and transmit cell counts for each connection.
interface <i>interface</i>	(Optional)	Displays only connections with an endpoint of the specified interface.
<i>vpi vci</i>	(Optional)	Displays only detailed information on the endpoint with the specified virtual path identifier (VPI)/virtual channel identifier (VCI) on the specified interface.
descriptor <i>descriptor</i>	(Optional)	Displays only connections with an endpoint on the interface with the specified physical descriptor.

Command Modes	
	User EXEC
	Privileged EXEC

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

Examples Each connection is listed twice in the output from the **show xtagatm cross-connect** command, because it shows each interface that is linked by the connection.

The following is sample output from the **show xtagatm cross-connect** command:

```
Router# show xtagatm cross-connect
```

Phys Desc	VPI/VCI	Type	X-Phys Desc	X-VPI/VCI	State
10.1.0	1/37	->	10.3.0	1/35	UP
10.1.0	1/34	->	10.3.0	1/33	UP
10.1.0	1/33	<->	10.2.0	0/32	UP
10.1.0	1/32	<->	10.3.0	0/32	UP
10.1.0	1/35	<-	10.3.0	1/34	UP
10.2.0	1/57	->	10.3.0	1/49	UP
10.2.0	1/53	->	10.3.0	1/47	UP
10.2.0	1/48	<-	10.1.0	1/50	UP
10.2.0	0/32	<->	10.1.0	1/33	UP
10.3.0	1/34	->	10.1.0	1/35	UP
10.3.0	1/49	<-	10.2.0	1/57	UP
10.3.0	1/47	<-	10.2.0	1/53	UP
10.3.0	1/37	<-	10.1.0	1/38	UP
10.3.0	1/35	<-	10.1.0	1/37	UP
10.3.0	1/33	<-	10.1.0	1/34	UP
10.3.0	0/32	<->	10.1.0	1/32	UP

Table 121 describes the significant fields shown in the display.

Table 121 show xtagatm cross-connect Field Descriptions

Field	Description
Phys desc	Physical descriptor. A switch-supplied string identifying the interface on which the endpoint exists.
VPI/VCI	Virtual path identifier and virtual channel identifier for this endpoint.
Type	The type can be one of the following: A right arrow (->) indicates an ingress endpoint, where traffic is received into the switch. A left arrow (<-) indicates an egress endpoint, where traffic is transmitted from the interface. A bidirectional arrow (<->) indicates that traffic is both transmitted and received at this endpoint.
X-Phys Desc	Physical descriptor for the interface of the other endpoint belonging to the cross-connect.
X-VPI/VCI	Virtual path identifier and virtual channel identifier of the other endpoint belonging to the cross-connect.
State	Indicates the status of the cross-connect to which this endpoint belongs. The state is typically UP; other values, all of which are transient, include the following: <ul style="list-style-type: none"> • DOWN • ABOUT_TO_DOWN • ABOUT_TO_CONNECT • CONNECTING • ABOUT_TO_RECONNECT • RECONNECTING • ABOUT_TO_RESYNC • RESYNCING • NEED_RESYNC_RETRY • ABOUT_TO_RESYNC_RETRY • RETRYING_RESYNC • ABOUT_TO_DISCONNECT • DISCONNECTING

The following is sample output from the **show xtagatm cross-connect** command for a single endpoint:

```
Router# show xtagatm cross-connect descriptor 10.1.0 1 42

Phys desc: 10.1.0
Interface: n/a
Intf type: switch control port
VPI/VCI: 1/42
X-Phys desc: 10.2.0
X-Interface: XTagATM0
X-Intf type: extended tag ATM
```

```

X-VPI/VCI:    2/38
Conn-state:   UP
Conn-type:    input/output
Cast-type:    point-to-point
Rx service type:  Tag COS 0
Rx cell rate:  n/a
Rx peak cell rate: 10000
Tx service type:  Tag COS 0
Tx cell rate:    n/a
Tx peak cell rate: 10000

```

Table 122 describes the significant fields shown in the display.

Table 122 show xtagatm cross-connect descriptor Field Descriptions

Field	Description
Phys desc	Physical descriptor. A switch-supplied string identifying the interface on which the endpoint exists.
Interface	The (Cisco IOS) interface name.
Intf type	Interface type. Can be either extended Multiprotocol Label Switched (MPLS) ATM (XTagATM) or a switch control port.
VPI/VCI	Virtual path identifier and virtual channel identifier for this endpoint.
X-Phys desc	Physical descriptor for the interface of the other endpoint belonging to the cross-connect.
X-Interface	The (Cisco IOS) name for the interface of the other endpoint belonging to the cross-connect.
X-Intf type	Interface type for the interface of the other endpoint belonging to the cross-connect.
X-VPI/VCI	Virtual path identifier and virtual channel identifier of the other endpoint belonging to the cross-connect.
Conn-state	Indicates the status of the cross-connect to which this endpoint belongs. The cross-connect state is typically UP; other values, all of which are transient, include the following: <ul style="list-style-type: none"> • DOWN ABOUT_TO_DOWN ABOUT_TO_CONNECT • CONNECTING • ABOUT_TO_RECONNECT • RECONNECTING • ABOUT_TO_RESYNC • RESYNCING • NEED_RESYNC_RETRY • ABOUT_TO_RESYNC_RETRY • RETRYING_RESYNC • ABOUT_TO_DISCONNECT • DISCONNECTING

Table 122 show xtagatm cross-connect descriptor Field Descriptions (continued)

Field	Description
Conn-type	<p>Input—Indicates an ingress endpoint where traffic is only expected to be received into the switch.</p> <p>Output—Indicates an egress endpoint, where traffic is only expected to be sent from the interface.</p> <p>Input/output—Indicates that traffic is expected to be both send and received at this endpoint.</p>
Cast-type	Indicates whether the cross-connect is multicast.
Rx service type	Quality of service type for the receive, or ingress, direction. This is MPLS QoS <n>, (MPLS Quality of Service <n>), where n is in the range from 0 to 7 for input and input/output endpoints; this will be N/A for output endpoints. (In the first release, this is either 0 or 7.)
Rx cell rate	(Guaranteed) cell rate in the receive, or ingress, direction.
Rx peak cell rate	Peak cell rate in the receive, or ingress, direction, in cells per second. This is n/a for an output endpoint.
Tx service type	Quality of service type for the transmit, or egress, direction. This is MPLS QoS <n>, (MPLS Class of Service <n>), where n is in the range from 0 to 7 for output and input/output endpoints; this will be N/A for input endpoints.
Tx cell rate	(Guaranteed) cell rate in the transmit, or egress, direction.
Tx peak cell rate	Peak cell rate in the transmit, or egress, direction, in cells per second. This is N/A for an input endpoint.

show xtagatm vc

To display information about terminating virtual circuits (VCs) on extended Multiprotocol Label Switching (MPLS) ATM (XTagATM) interfaces, use the **show xtagatm vc** command in user EXEC or privileged EXEC mode.

```
show xtagatm vc [vcd [interface]]
```

Syntax Description

<i>vcd</i>	(Optional) Virtual circuit descriptor (virtual circuit number). If you specify the <i>vcd</i> argument, information displays about all VCs with that virtual circuit descriptor (VCD). If you do not specify the <i>vcd</i> argument, a summary description of all VCs on all XTagATM interfaces displays.
<i>interface</i>	(Optional) Interface number. If you specify the <i>interface</i> and the <i>vcd</i> arguments, information displays about the specified VC on the specified interface.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

The columns marked VCD, VPI, and VCI display information for the corresponding private VC on the control interface. The private VC connects the XTagATM VC to the external switch. It is termed private because its VPI and VCI are only used for communication between the MPLS LSC and the switch, and it is different from the VPI and VCI seen on the XTagATM interface and the corresponding switch port.

Examples

Each connection is listed twice in the sample output from the **show xtagatm vc cross-connect** command under each interface that is linked by the connection. Connections are marked as input (unidirectional traffic flow, into the interface), output (unidirectional traffic flow, away from the interface), or in/out (bidirectional).

The following is sample output from the **show xtagatm vc** command:

```
Router# show xtagatm vc
```

```
AAL / Control Interface
Interface      VCD  VPI  VCI Type  Encapsulation  VCD  VPI  VCI Status
XTagATM0      1    0   32  PVC   AAL5-SNAP      2    0   33 ACTIVE
XTagATM0      2    1   33  TVC   AAL5-MUX       4    0   37 ACTIVE
XTagATM0      3    1   34  TVC   AAL5-MUX       6    0   39 ACTIVE
```

Table 123 describes the significant fields shown in the display.

Table 123 *show xtagatm vc* Field Descriptions

Field	Description
VCD	Virtual circuit descriptor (virtual circuit number).
VPI	Virtual path identifier.
VCI	Virtual circuit identifier.
Control Interf. VCD	VCD for the corresponding private VC on the control interface.
Control Interf. VPI	VPI for the corresponding private VC on the control interface.
Control Interf. VCI	VCI for the corresponding private VC on the control interface.
Encapsulation	Displays the type of connection on the interface.
Status	Displays the current state of the specified ATM interface.

Related Commands

Command	Description
<code>show atm vc</code>	Displays information about private ATM VCs.
<code>show xtagatm cross-connect</code>	Displays information about remotely connected ATM switches.

snmp-server enable traps mpls ldp

To enable the sending of Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps mpls ldp** command in global configuration mode. To disable the sending of MPLS LDP notifications, use the **no** form of this command.

snmp-server enable traps mpls ldp [session-up | session-down | pv-limit | threshold]

no snmp-server enable traps mpls ldp [session-up | session-down | pv-limit | threshold]

Syntax Description	
session-up	(Optional) Controls (enables or disables) LDP session up notifications, defined in the MPLS-LDP-MIB as mplsLdpSessionUp. This notification is generated when the router establishes an LDP session with another LDP entity (an adjacent LDP peer in the network).
session-down	(Optional) Controls (enables or disables) LDP session down notifications, defined in the MPLS-LDP-MIB as mplsLdpSessionDown. This message is generated when an LDP session between the router and its adjacent LDP peer is terminated.
pv-limit	(Optional) Controls (enables or disables) Path-Vector (PV) Limit notifications, defined in the MPLS-LDP-MIB as mplsLdpPVLMismatch. This notification is generated when the router establishes an LDP session with its adjacent peer label switch router (LSR), but the two LSRs have dissimilar path vector limits.
threshold	(Optional) Controls (enables or disables) PV Limit notifications, defined in the MPLS-LDP-MIB as mplsLdpInitSesThresholdExceeded. This notification is generated after eight failed attempts to establish an LDP session between the router and an LDP peer, due to any type of incompatibility between the devices.

Defaults

The sending of SNMP notifications is disabled by default.

If you do not specify any of the optional keywords, all four types of LDP notifications are enabled on the LSR.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The MPLS LDP **pv-limit** (mplsLdpPathVectorLimitMismatch) notification object provides a warning message that can be sent to the NMS when two routers engaged in LDP operations have a dissimilar path vector limit. It is recommended that all LDP-enabled routers in the network be configured with the same path vector limit.

The value of the path vector limit can range from 0 through 255; a value of 0 indicates that loop detection is off; any value other than zero up to 255 indicates that loop detection is on and, in addition, specifies the maximum number of hops through which an LDP message can pass before a loop condition in the network is sensed.

The MPLS LDP **threshold** (mplsLdpFailedInitSessionThresholdExceeded) notification object provides a warning message that can be sent to a network management station (NMS) when a local LSR and an adjacent LDP peer attempt to set up an LDP session between them, but fail to do so after a specified number of attempts. The default number of attempts is 8. This default value is implemented in Cisco IOS and cannot be changed using either the CLI or an SNMP agent.

In general, Cisco routers support the same features across multiple platforms. Therefore, the most likely incompatibility to occur between Cisco LSRs is a mismatch of their respective ATM VPI/VCI label ranges.

For example, if you specify a range of valid labels for an LSR that does not overlap the range of its adjacent LDP peer, the routers will try eight times to create an LDP session between themselves before the mplsLdpFailedInitSessionThresholdExceeded notification is generated.

Operationally, the LSRs whose label ranges do not overlap continue their attempt to create an LDP session between themselves after the eight retry threshold is exceeded. In such cases, the LDP threshold exceeded notification alerts the network administrator to the existence of a condition in the network that may warrant attention.

RFC 3036, *LDP Specification*, details the incompatibilities that can exist between Cisco routers and/or other vendor LSRs in an MPLS network. Among such incompatibilities, for example, are the following:

- Non-overlapping ATM VPI/VCI ranges (as noted above) or non-overlapping Frame-Relay DLCI ranges between LSRs attempting to set up an LDP session
- Unsupported label distribution method
- Dissimilar protocol data unit (PDU) size
- Dissimilar LDP feature support

The **snmp-server enable traps mpls ldp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable LDP-specific informs that will be sent to the host myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps mpls ldp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public mpls-ldp
```

snmp-server enable traps mpls traffic-eng

To enable Multiprotocol Label Switching (MPLS) traffic engineering tunnel state-change Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps mpls traffic-eng** command in global configuration mode. To disable MPLS traffic engineering tunnel state-change SNMP notifications, use the **no** form of this command.

snmp-server enable traps mpls traffic-eng [up | down | reroute]

no snmp-server enable traps mpls traffic-eng [up | down | reroute]

Syntax Description	
up	(Optional) Enables only mplsTunnelUp notifications { mplsTeNotifyPrefix 1 }. MplsTunnelUp notifications are sent to a network management system (NMS) when an MPLS traffic engineering tunnel is configured and the tunnel transitions from an operationally “down” state to an “up” state.
down	(Optional) Enables only mplsTunnelDown notifications { mplsTeNotifyPrefix 2 }. MplsTunnelDown notifications are generated and sent to the NMS when an MPLS traffic engineering tunnel transitions from an operationally “up” state to a “down” state.
reroute	(Optional) Controls (enables or disables) only mplsTunnelRerouted notifications { mplsTeNotifyPrefix 3 }. MplsTunnelRerouted notifications are sent to the NMS under the following conditions: 1) The signaling path of an existing MPLS traffic engineering tunnel fails for some reason and a new path option is signaled and placed into effect (that is, the tunnel is rerouted). or 2) The signaling path of an existing MPLS traffic engineering tunnel is fully operational, but a better path option can be signaled and placed into effect (that is, the tunnel can be reoptimized). This reoptimization can be triggered by: a) a timer, b) the issuance of an mpls traffic-eng reoptimize command, or c) a configuration change that requires the resignalling of a tunnel.

Defaults

SNMP notifications are disabled by default.

If this command is used without keywords, all available trap types (up, down, reroute) are enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) MPLS traffic engineering tunnel notifications. MPLS Tunnel StateChange notifications, when enabled, will be sent when the connection moves from an “up” to “down” state, when a connection moves from a “down” to “up” state, or when a connection is rerouted.

If you do not specify a specific argument in conjunction with this command, all three types of MPLS traffic engineering tunnel notifications will be sent.

The **snmp-server enable traps mpls traffic-eng** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable the router to send MPLS notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps mpls traffic-eng
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps mpls vpn

To enable the router to send Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) specific Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps mpls vpn** command in global configuration mode. To disable MPLS VPN specific SNMP notifications, use the **no** form of this command.

```
snmp-server enable traps mpls vpn [vrf-up] [vrf-down] [mid-threshold] [max-threshold]
[illegal-label]
```

```
no snmp-server enable traps mpls vpn [vrf-up] [vrf-down] [mid-threshold] [max-threshold]
[illegal-label]
```

Syntax Description	
vrf-up	(Optional) Enables a notification for the assignment of a VPN routing/forwarding instance (VRF) to an interface that is operational or for the transition of a VRF interface to the operationally up state.
vrf-down	(Optional) Enables a notification for the removal of a VRF from an interface or the transition of an interface to the down state.
mid-threshold	(Optional) Enables a notification of a warning that the number of routes created has crossed the warning threshold. This warning is sent only at the time the warning threshold is exceeded. The warning threshold value is a percentage of the max-threshold value, and is set using the maximum routes limit warn-threshold VRF configuration mode command.
max-threshold	(Optional) Enables a notification that the maximum route limit (maximum route threshold) has been reached. Another notification is sent when the number of routes falls below the maximum route limit value. The max-threshold value is determined by the maximum routes VRF configuration mode command.
illegal-label	(Optional) Enables a notification for any illegal labels received on a VRF interface. Labels are illegal if they are outside the legal range, do not have a Label Forwarding Information Base (LFIB) entry, or do not match table IDs for the label.

Defaults This command is disabled by default.

Command Modes Global 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.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines If this command is used without any of the optional keywords, all MPLS VPN notification types are enabled.

For the **vrf-up** (mplsVrfIfUp) or **vrf-down** (mplsVrfIfDown) notifications to be issued from an ATM or Frame Relay subinterface, you must first configure the **snmp-server traps atm subif** command or the **snmp-server traps frame-relay subif** command on the subinterfaces, respectively.

The values for **mid-threshold** and **max-threshold** are set using the **maximum routes limit warn-threshold [warn-only]** VRF configuration mode command.

**Note**

The **warn-only** keyword in the **maximum routes** command sets the value of the MaxThreshold object to an effectively infinite number, so MaxThreshExceeded (**max-threshold**) SNMP notifications will never be sent for the configured VRF if the **maximum routes limit warn-only** command is used. In other words, the **maximum routes limit warn-only** command will generate syslog messages when the limit value (max-threshold) is reached, but SNMP notifications will not be generated.

The notification types described above are defined in the following MIB objects of the PPVPN-MPLS-VPN-MIB as follows:

- mplsVrfIfUp
- mplsVrfIfDown
- mplsNumVrfRouteMidThreshExceeded
- mplsNumVrfRouteMaxThreshExceeded
- mplsNumVrfSecIllegalLabelThreshExceeded

Examples

The following example shows how to send MPLS VPN trap notifications to the host specified as 172.31.156.34 using the community string named public if a VRF transitions from a down state to an up state or from an up state to a down state:

```
Router(config)# snmp-server enable traps mpls vpn vrf-up vrf-down
Router(config)# snmp-server host 172.31.156.34 traps public mpls-vpn
```

Related Commands

Command	Description
maximum routes	Sets the warning threshold and route maximum for VRFs.
snmp-server traps atm subif	Enables ATM Subinterface SNMP notifications.
snmp-server traps frame-relay subif	Enables Frame-Relay Subinterface SNMP notifications.
snmp-server host	Specifies the recipient of SNMP notifications.

spanning-tree cost

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

spanning-tree cost *cost*

no spanning-tree cost

Syntax Description

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

Defaults

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

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

Command Modes

Interface configuration

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 family switches.
12.1(3a)E	This command was modified to support 32-bit path cost.
12.2(2)XT	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

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

Examples

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

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

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

spanning-tree port-priority

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

spanning-tree port-priority *port-priority*

no spanning-tree port-priority

Syntax Description

port-priority Port priority; valid values are from 2 to 255. The default is 128.

Defaults

The port priority is 128.

Command Modes

Interface 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

The priority you set breaks the tie.

Examples

The following example shows how to increase the likelihood that the spanning tree instance 20 is chosen as the root-bridge on interface ethernet 2/0:

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

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree state information.
spanning-tree cost	Sets the path cost of the interface for STP calculations.
spanning-tree portfast (global configuration mode)	Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire.

Command	Description
spanning-tree portfast (interface configuration mode)	Enables PortFast mode, which places the interface immediately into the forwarding state upon linkup without waiting for the timer to expire.
spanning-tree uplinkfast	Enables the UplinkFast feature.
spanning-tree vlan	Configures STP on a per-VLAN basis.

spanning-tree vlan

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

```
spanning-tree vlan vlan-id [forward-time seconds | hello-time seconds | max-age seconds |
priority priority | protocol protocol | [root {primary | secondary}] [diameter net-diameter
hello-time seconds]]]
```

```
no spanning-tree vlan vlan-id [forward-time | hello-time | max-age | priority | protocol | root]
```

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

Defaults

forward-time: 15 seconds
hello-time: 2 seconds
max-age: 20 seconds
priority: The default with IEEE STP enabled is 32,768; with STP enabled, the default is 128.
protocol: IEEE
root: No STP root

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.
	12.2(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 setting the **max-age** *seconds*, if a bridge does not hear Bridge Protocol Data Units (BPDU) from the root bridge within the specified interval, it assumes that the network has changed and recomputes the spanning tree topology.

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

The **spanning-tree root primary** command alters this switch's bridge priority to 8,192. If you enter after **spanning-tree root primary** command and the switch does not become root, then the bridge priority is changed to 100 less than the bridge priority of the current bridge. If the switch does not become root, an error results.

The **spanning-tree root secondary** command alters this switch's bridge priority to 16,384. If the root switch should fail, this switch becomes the next root switch.

Use the **spanning-tree root** commands on backbone switches only.

Examples

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

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

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

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

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

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

Related Commands	Command	Description
	show spanning-tree	Displays spanning-tree state information.
	spanning-tree cost	Sets the path cost of the interface for STP calculations.
	spanning-tree port-priority	Sets an interface priority when two bridges tie for position as the root bridge.
	spanning-tree portfast (global configuration mode)	Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup, without waiting for the timer to expire.
	spanning-tree portfast (interface configuration mode)	Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup, without waiting for the timer to expire.
	spanning-tree uplinkfast	Enables the UplinkFast feature.

tag-control-protocol vsi

To configure the use of Virtual Switch Interface (VSI) on a particular master control port, use the **tag-control-protocol vsi** command in interface configuration mode. To disable VSI, use the **no** form of this command.

```
tag-control-protocol vsi [id controller-id] [base-vc vpi vci] [slaves slave-count]
[keepalive timeout] [retry timeout-count] [delay seconds]
```

```
no tag-control-protocol vsi [id controller-id] [base-vc vpi vci] [slaves slave-count]
[keepalive timeout] [retry timeout-count] [delay seconds]
```

Syntax Description

id <i>controller-id</i>	(Optional) Determines the value of the controller-id field present in the header of each VSI message. The default is 1.
base-vc <i>vpi vci</i>	(Optional) Determines the VPI/VCI value for the channel to the first slave. The default is 0/40. Together with the slave value, this value determines the VPI/VCI values for the channels to all of the slaves, which are as follows: <ul style="list-style-type: none"> <i>vpi/vci</i> <i>vpi/vci</i>+1, and so on <i>vpi/vci</i>+<i>slave-count</i>-1
slaves <i>slave-count</i>	(Optional) Determines the number of slaves reachable through this master control port. The default is 14 (suitable for the Cisco BPX switch).
keepalive <i>timeout</i>	(Optional) Determines the value of the keepalive timer (in seconds). Make sure that the keepalive timer value is greater than the value of the retry timer times the retry timer +1. The default is 15 seconds.
retry <i>timeout-count</i>	(Optional) Determines the value of the message retry timer (in seconds) and the maximum number of retries. The default is 8 seconds and 10 retries.
delay <i>seconds</i>	(Optional) Specifies the delay time to start a new VSI session after the system comes up or after you enter the command. If a VSI session is already running, the delay keyword has no effect for the current session. The delay is implemented when a new VSI session starts. The default is 0. The valid range of values is 0 to 300.

Defaults

VSI is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(15)T	The delay keyword was added.

Usage Guidelines

The command is only available on interfaces that can serve as a VSI master control port. We recommend that all options to the **tag-control-protocol vsi** command be entered at the same time.

After VSI is active on the control interface (through the earlier issuance of a **tag-control-protocol vsi** command), reentering the command may cause all associated XTagATM interfaces to shut down and restart. In particular, if you reenter the **tag-control-protocol vsi** command with any of the following options, the VSI shuts down and reactivates on the control interface:

- **id**
- **base-vc**
- **slaves**

VSI remains continuously active (that is, the VSI does not shut down and then reactivate) if you reenter the **tag-control-protocol vsi** command with only one or both of the following options:

- **keepalive**
- **retry**
- **delay**

In either case, if you reenter the **tag-control-protocol vsi** command, this causes the specified options to take on the newly specified values; the other options retain their previous values. To restore default values to all the options, enter the **no tag-control-protocol** command, followed by the **tag-control-protocol vsi** command.

Examples

The following example shows how to configure the VSI driver on the control interface:

```
Router(config)# interface atm 0/0  
Router(config-if)# tag-control-protocol vsi base-vc 0 51
```

tag-switching advertise-tags

The **tag-switching advertise-tags** command is replaced by the **mpls advertise-labels** command. See the [mpls ldp advertise-labels](#) command for more information.

tag-switching atm allocation-mode

The **tag-switching atm allocation-mode** command is replaced by the **mpls ldp atm control-mode** command. See the [mpls ldp atm control-mode](#) command for more information.

tag-switching atm cos

The **tag-switching atm cos** command is replaced by the **mpls atm cos** command. See the [mpls atm cos](#) command for more information.

tag-switching atm disable-headend-vc

The **tag-switching atm disable-headend-vc** command is replaced by the **mpls atm disable-headend-vc** command. See the [mpls atm disable-headend-vc](#) command for more information.

tag-switching atm maxhops

The **tag-switching atm maxhops** command is replaced by the **mpls ldp maxhops** command. See the [mpls ldp maxhops](#) command for more information.

tag-switching atm vc-merge

The **tag-switching atm vc-merge** command is replaced by the **mpls atm vc-merge** command. See the [mpls ldp atm vc-merge](#) command for more information.

tag-switching atm vpi

The **tag-switching atm vpi** command is replaced by the **mpls atm vpi** command. See the [mpls atm vpi](#) command for more information.

tag-switching atm vp-tunnel

The **tag-switching atm vp-tunnel** command is replaced by the **mpls atm vp-tunnel** command. See the [mpls atm vp-tunnel](#) command for more information.

tag-switching cos-map

The **tag-switching cos-map** command is replaced by the **mpls cos-map** command. See the [mpls cos-map](#) command for more information.

tag-switching prefix-map

The **tag-switching prefix-map** command is replaced by the **mpls prefix-map** command. See the [mpls prefix-map](#) command for more information.

tag-switching request-tags for

The **tag-switching request-tags for** command is replaced by the **mpls request-labels for** command. See the [mpls request-labels for](#) command for more information.

tag-switching tdp discovery

The **tag-switching tdp discovery** command is replaced by the **mpls ldp discovery** command. See the [mpls ldp discovery](#) command for more information.

tag-switching tdp holdtime

The **tag-switching tdp holdtime** command is replaced by the **mpls ldp holdtime** command. See the [mpls ldp holdtime](#) command for more information.