Configuring the OC-12 ATM Optical Services Modules

This chapter describes the 2-port OC-12 ATM WAN Optical Services Modules (OSMs).

This chapter consists of these sections:

- ATM Overview, page 8-1
- Supported Features, page 8-2
- Configuring the OC-12 ATM Interfaces, page 8-3
- Configuring Virtual Connections, page 8-6
- Configuring Automatic Protection Switching, page 8-26
- SONET and SDH Configuration Commands, page 8-31

ATM Overview

Asynchronous Transfer Mode (ATM) uses cell-switching and multiplexing technology that combines the benefits of circuit switching (constant transmission delay and guaranteed capacity) with the benefits of packet switching (flexibility and efficiency for intermittent traffic).

ATM is a connection-oriented environment. All traffic to or from an ATM network is prefaced with a virtual path identifier (VPI) and virtual channel identifier (VCI). A VPI/VCI pair is considered a single virtual circuit. Each virtual circuit is a private connection to another node on the ATM network. Each virtual circuit is treated as a point-to-point mechanism to another router or host and can support bidirectional traffic.

Each ATM node is required to establish a separate connection to every other node in the ATM network that it must communicate with. All such connections are established using a permanent virtual circuit (PVC), which a network operator configures, or a switched virtual circuit (SVC), which is set up and torn down with an ATM signaling mechanism. This signaling is based on the ATM Forum User-Network Interface (UNI) specification V3.x, 4.0.

Supported Features

The WAN ports on the 2-port OC-12 ATM OSMs support the following features:

- Multiprotocol label switching (MPLS) VPNs
- Permanent virtual circuits (PVCs)
- Switched virtual circuits (SVCs); up to 100 SVCs
- Maximum of 1000 VCs per module; 500 per physical ATM interface
- VPI range 0 through 255 (the default is 15)
- VCI range 1 through 1023 (the default is 1023)
- RFC 1577 classical IP over ATM
- RFC 1483 bridging support for PVCs only
- Bridging of 1483 Routed Encapsulations (BRE)
- Hardware switching of multicast packets on point-to-point subinterfaces
- Software switching of multicast packets on point-to-multipoint subinterfaces
- UNI 3.x and UNI 4.0
- ILMI 1.0
- Per-VC Layer 3 queuing
- Layer 3 traffic shaping
  - CIR
  - EIR
- PFC QoS with OSM-2OC12-ATM-MM/SI+
- Per-VP shaping
- Per-VC shaping
- UBR and VBR-NRT
- Per-VC class-based weighted fair queuing (CBWFQ)
- Low latency queuing (LLQ)
- Weighted Random Early Detection (WRED)
- Committed Access Rate (CAR)
- SONET Linear APS 1+1
- Multipoint Bridging
- PVST+ to 802.1d BPDU conversion

Note For the OC-12 ATM OSM, the Common Part Convergence Sublayer User-to-User (CPCS-UU) field in the AAL5 CPCS PDU cannot be set, cleared, or transported correctly. This affects custom use of the field as well as FRF8.1, which uses the CPCS-UU byte to transport the Frame Relay command response (C/R) bit.

For QoS configuration information and examples for the WAN OSM ports, see the "Configuring QoS on the OSMs" section on page 9-2.

For MPLS QoS configuration information and examples for the WAN OSM ports, see the "Configuring MPLS QoS" section on page 11-13.

For general information on how to configure Cisco IOS QoS, refer to these Cisco IOS publications:

Cisco IOS Quality of Service Solutions Configuration Guide at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/index.htm

Cisco IOS Quality of Service Solutions Command Reference at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_r/index.htm

Configuring the OC-12 ATM Interfaces

This section provides procedures for initial configuration of an OC-12 ATM OSM interface:

- Initial Configuration for the OC-12 ATM OSM, page 8-3
- Enabling the ATM Interface, page 8-3
- Valid VCI and VPI Configurations, page 8-4

Initial Configuration for the OC-12 ATM OSM

On power-on, the interfaces on a new OC-12 ATM OSM are shut down. To enable an interface, you must enter the **no shutdown** command in configuration mode. When the OC-12 ATM interface is enabled with no additional configuration, the default interface configuration file parameters are used. These default parameters are listed in Table 8-1.

Table 8-1 OC-12c/STM-4c ATM Module Configuration Default Values

Parameter	Configuration Command	Default Value
Maximum transmission unit	[**no**] **mtu** *bytes*	4470 bytes
Loopback	[**no**] **loopback** [**diagnostic** | **line**]	no loopback
ATM VCs per VP	**atm vc-per-vp**	1023

After you verify that the new OC-12 ATM module is installed correctly (the active LED goes on and all cables are correctly connected), you can use the **configure** command to configure the ATM interfaces.

Enabling the ATM Interface

A Cisco Catalyst 6000 family switch and Cisco 7600 series router identifies an interface address by its slot number and port number in the format *slot/port*. For example, the slot/port address of an interface on a 2-port OC-12 ATM OSM installed in slot 4 is 4/1.

Before using the **configure** command, you must enter the privileged level mode of the EXEC command interpreter by using the **enable** command. The system prompts you for a password if one is set.

Use the following procedure to configure the 2-port OC-12 ATM OSMs. Press the **Return** key after each configuration step unless otherwise noted.

To configure the ATM interfaces, perform this task:

	Command	Purpose
Step 1	`Router# show module`	Confirms that the system recognizes the module.
Step 2	`Router# show interface atm slot/port`	Checks the status of each port.
Step 3	`Router# configure terminal`	Enters configuration mode and specifies that the console terminal is the source of configuration subcommands.
Step 4	`Router(config)# interface atm slot/port`	Specifies the new interface to configure.
Step 5	`Router(config-if)# ip address ip-address mask [secondary]`	Assigns an IP address and subnet mask to the interface.
Step 6	`Router(config-if)# no shutdown` `Router(config-if)# end`	Changes the interface state to up and enables the interface.
Step 7	`Router# copy running-config startup-config`	Writes the new configuration to memory.

This example shows how to configure an OC-12 ATM OSM interface:

```
Router# configure terminal
Router(config)# interface atm 4/0
Router(config-if)# ip address 1.2.3.4 255.255.255.0
Router(config-if)# no shutdown
Router# copy running-config startup-config
```

Valid VCI and VPI Configurations

The default number of VPIs per ATM interface is 15. The maximum number of VCIs per VPI is 1023.

Table 8-2 shows the valid VCs per VP and maximum VPI configurations.

Table 8-2 Valid VCI and VPI Configurations

VCs per VP	Maximum VPIs
1024	15
512	31
256	63
128	127
64	255
32	255
16	255

Configuring the Maximum VCs per VP

The ATM interfaces are configured by default to allow a maximum of 1023 VCs per VP. To change this value, perform this task beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface atm slot/port`	Enters interface configuration mode and specifies the ATM interface to configure.
Step 2	`Router(config-if)# atm vc-per-vp`	Configures the maximum number of VCs per VP to 16, 32, 64, 128, 256, 512, or 1024. The default is 1024.
Step 3	`Router(config-if)# no shutdown`	Enables the interface with the above configuration.

Configuring Virtual Connections

This section provides basic information for configuring PVCs, bridged PVCs (RFC 1483), PVC traffic parameters, and SVCs. In addition, this section documents commands and configurations that are unique to the 2-port OC-12 ATM OSMs.

- Creating a PVC, page 8-6
- Configuring Bridging of RFC 1483 Routed Encapsulations, page 8-7
- Configuring PVC Traffic Parameters, page 8-9
- Configuring SVCs, page 8-9
- Configuring Multipoint Bridging, page 8-13
- RFC 1483 Spanning-Tree Interoperability Enhancements, page 8-18

For all other Cisco IOS features and commands supported on the OC-12 ATM OSMs, refer to the "Configuring ATM" chapter in the *Cisco IOS Wide-Area Networking Configuration Guide,* Release 12.1 at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/wan_c/wcdatm.htm

For complete command syntax information, refer to the "ATM commands" chapter in the *Cisco IOS Wide-Area Networking Command Reference,* Release 12.1 at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/wan_r/wratm/index.htm

Creating a PVC

To create a PVC on the ATM interface and enter interface-ATM-VC configuration mode, perform this task in interface configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface atm slot/port`	Specifies the new interface to configure.
Step 2	`Router(config-if)# ip address ip-address mask [secondary]`	Assigns an IP address and subnet mask to the interface.
Step 3	`Router(config-if)# pvc [name] vpi/vci [ilmi | qsaal]`	Configures a new ATM PVC by assigning a name (optional) and VPI/VCI numbers. Enters interface-ATM-VC configuration mode. Optionally configures ILMI or QSAAL encapsulation.
Step 4	`Router(config-if-atm-vc)# protocol protocol protocol-address [[no] broadcast]`	Maps a protocol address to a PVC.
Step 5	`Router(config-if-atm-vc)# encapsulation {aal5mux | aal5snap}`	(Optional) Configures the ATM adaptation layer (AAL) and encapsulation type. The default is **aal5snap**.

This example shows how to create a PVC:

```
Router(config)# interface atm 4/0
Router(config-if)# ip address 10.212.13.4 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# pvc cisco 0/56
Router(config-if-atm-vc)# protocol ip 10.212.13.5 broadcast
Router(config-if-atm-vc)# encapsulation aal5snap
Router(config-if-atm-vc)#
```

Configuring Bridging of RFC 1483 Routed Encapsulations

Bridging of routed encapsulations (BRE) enables the OC-12 ATM OSM to receive RFC 1483 routed encapsulated packets and forward them as Layer 2 frames.

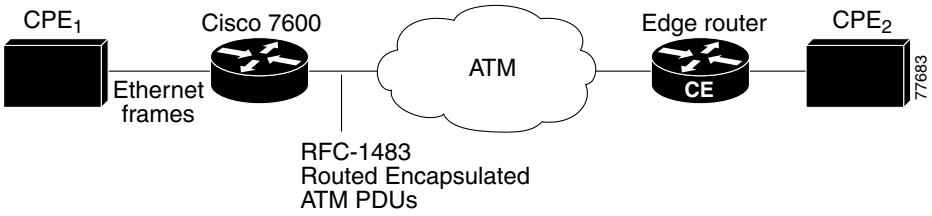
Note Concurrent configuration of RFC 1483 bridging and BRE on the same PVC and VLAN is not supported.

When you configure BRE on an ATM PVC on the OC-12 ATM OSM:

1. The PVC receives the routed PDUs,
2. The PVC removes the RFC 1483 routed encapsulation header,
3. The PVC adds an Ethernet MAC header to the packet.
4. The supervisor engine then switches the Layer 2 encapsulated packet to the Layer 2 interface determined by the VLAN number and destination MAC.

Figure 8-1 shows a topology in which an OC-12 ATM OSM receives routed PDUs, encapsulates them as Layer 2 frames, and forwards these frames to a Layer 2 customer device.

Figure 8-1 Example BRE Topology



To configure BRE on a PVC, use the following commands:

	Command	Purpose
Step 1	`Router(config)# vlan`	Configures the Layer 2 VLAN.
Step 2	`Router(config)# interface atm slot/port [.subinterface-number point-to-point]`	Specifies the subinterface on which to configure the PVC.
Step 3	`Router(config-subif)# pvc [name] vpi/vci`	Configures a new ATM PVC by assigning a name (optional) and VPI/VCI numbers.
Step 4	`Router(config-if-atm-vc)# bre-connect vlan [ip ip address]`	Enables BRE on the PVC. Using the **ip** keyword allows the BRE device to generate an ARP request to learn the CPE MAC address the first time a packet needs to be sent from the BRE switch to the CPE.

	Command	Purpose
Step 5	`Router(config)# interface GigabitEthernet slot/port`	Specifies the Gigabit Ethernet port to configure.
Step 6	`Router(config-if)# switchport`	Configures the Gigabit Ethernet port for Layer 2 switching.
Step 7	`Router(config-if)# switchport access vlan vlan_id`	(Optional) Specifies the default VLAN, which is used if the interface stops trunking.
Step 8	`Router(config-if)# switchport mode access`	Places the interface into nontrunking mode.

Step 1 Configure the Layer 2 VLAN.

```
Router# configure terminal
Router(config)# vlan 10
Router(config-vlan)# exit
```

Step 2 Configure the VLAN interface:

```
Router(config)# interface vlan 10
Router(config-if)# no shutdown
Router(config-if)# end
Router#
```

Step 3 Configure the default VLAN on the Ethernet interface:

```
Router(config)# interface GigabitEthernet3/3
Router(config-if)# no ip address
Router(config-if)# switchport
Router(config-if)# switchport access vlan 10
Router(config-if)# switchport mode access
Router(config-if)# end
Router#
```

Step 4 Enable the ATM main interface:

```
Router(config)# interface atm3/1
Router(config-if)# no ip address
Router(config-if)# no shutdown
Router(config-if)# end
Router#
```

Step 5 Configure the PVC:

```
Router(config)# interface atm3/1.1 point-to-point
Router(config-if)# no ip address
Router(config-subif)# mtu 1500
Router(config-subif)# pvc 1/101
Router(config-if-atm-vc)# bre-connect 10
Router(config-subif)# end
Router#
```

Note If an ATM interface has only BRE VLANs configured, you must enter the **spanning-tree bpdufilter enable** command on the main ATM interface. Entering this command blocks all spanning tree BPDUs on the ATM interface. If RFC 1483 bridged VLANs are also configured on the same ATM interface or on one of its subinterfaces, do not enter the **spanning-tree bpdufilter enable** command unless you want to specifically block BPDUs on that interface.

Configuring PVC Traffic Parameters

The supported traffic parameters are part of the following service categories: Unspecified Bit Rate (UBR) and Variable Bit Rate Non Real-Time (VBR-NRT). Only one of these categories can be specified per PVC connection; if a new one is entered, it replaces the existing one.

To configure PVC traffic parameters, perform one of these tasks beginning in interface-ATM-VC configuration mode:

Command	Purpose
`Router(config-if-atm-vc)# ubr`	Configures UBR. The default is UBR.
`Router(config-if-atm-vc)# vbr-nrt` *pcr scr mbs*	Configures VBR-NRT.

The *-pcr*, *-scr,* and *-mbs* arguments are the peak cell rate, sustainable cell rate, and maximum burst size.

The maximum configurable speed of a VBR-NRT PVC is 299520 Mbps. The maximum MBS is 255 cells.

This example shows how to configure VBR-NRT with a peak cell rate of 1000, a sustainable cell rate of 500, and a maximum burst size of 64:

```
Router(config-if-atm-vc)# vbr-nrt 1000 500 64
Router(config-if-atm-vc)#
```

Configuring SVCs

ATM SVCs are created and released dynamically, providing user bandwidth on demand. This service requires a signaling protocol between the router and the switch.

The ATM signaling software provides a method of dynamically establishing, maintaining, and clearing ATM connections at the UNI. The ATM signaling software conforms to ATM Forum UNI 3.x, 4.0 depending on the version selected by the ILMI or the configuration.

In UNI mode, the Cisco 7600 series router does not perform ATM-level call routing. Instead, the ATM switch performs the ATM call routing, and the router routes packets through the resulting circuit. The router is viewed as the user and the LAN interconnection device at the end of the circuit, and the ATM switch is viewed as the network.

You must complete the tasks in the following sections to use SVCs:

- Configuring Communication with the ILMI, page 8-9 (Required)
- Configuring the PVC that Performs SVC Call Setup, page 8-10 (Required)
- Configuring the NSAP Address, page 8-11 (Required)
- Creating an SVC, page 8-12 (Optional)

Configuring Communication with the ILMI

In an SVC environment, you must configure a PVC for communication with the Integrated Local Management Interface (ILMI) so the router can receive SNMP traps and new network prefixes. The recommended vpi and vci values for the ILMI PVC are 0 and 16, respectively. To configure ILMI communication, perform the following task in interface configuration mode:

Command	Purpose
Router(config-if)# **pvc** [*name*] *vpi*/*vci* [**ilmi** | **qsaal**]	Creates an ILMI PVC on an ATM main interface.

This example shows how to create an ILMI PVC on an ATM main interface:

```
Router(config-if)# pvc cisco 0/16 ilmi
```

Note This ILMI PVC can be set up only on an ATM main interface, not on ATM subinterfaces.

After you configure an ILMI PVC, you can optionally enable the ILMI keepalive function by performing the following task in interface configuration mode:

Command	Purpose
Router(config-if)# **atm ilmi-keepalive** [*seconds*]	Enables ILMI keepalives and sets the interval between keepalives.

ILMI address registration for receipt of SNMP traps and new network prefixes is enabled by default. The ILMI keepalive function is disabled by default; when enabled, the default interval between keepalives is 3 seconds.

This example shows how to set the ILMI keepalive interval to 3 minutes:

```
Router(config-if)# atm ilmi-keepalive 180
```

Configuring the PVC that Performs SVC Call Setup

One dedicated PVC exists between the router and the ATM switch, over which all SVC call-establishment and call-termination requests flow. After the call is established, data transfer occurs over the SVC, from router to router.

Before any SVCs can be set up, a signaling PVC must be configured.

To configure the signaling PVC for all SVC connections, perform this task in interface configuration mode:

Command	Purpose
Router(config-if)# **pvc** [*name*] *vpi*/*vci* [**ilmi** | **qsaal**]	Configures the signaling PVC for an ATM main interface that uses SVCs.

This example shows how to configure the signaling PVC:

```
Router(config-if)# pvc 0/5 qsaal
Router(config-if-atm-vc)#
```

Note This signaling PVC can be set up only on an ATM main interface, not on ATM subinterfaces.

The VPI and VCI values must be configured consistently with the ATM switch. The standard value for VPI is 0 and VCI is 5.

Configuring the NSAP Address

Each ATM interface involved with signaling must be configured with a network service access point (NSAP) address. The NSAP address is the ATM address of the interface and must be unique across the network.

To configure an NSAP address, complete the tasks described in one of the following sections:

- Configuring the ESI and Selector Fields, page 8-11
- Configuring the Complete NSAP Address, page 8-11

Configuring the ESI and Selector Fields

If the switch is capable of delivering the NSAP address prefix to the router by using ILMI, and the router is configured with a PVC for communication with the switch through ILMI, you can configure the end station ID (ESI) and selector fields using the **atm esi-address** command. The **atm esi-address** command allows you to configure the ATM address by entering the ESI (12 hexadecimal characters) and the selector byte (2 hexadecimal characters). The NSAP prefix (26 hexadecimal characters) is provided by the ATM switch.

To configure the router to get the NSAP prefix from the switch and use locally entered values for the remaining fields of the address, perform this task in Interface configuration mode:

	Command	Purpose
Step 1	`Router(config-if)# pvc [name] vpi/vci [ilmi | qsaal]`	Configures an ILMI PVC on an ATM main interface for communicating with the switch by using ILMI.
Step 2	`Router(config-if-atm-vc)# exit`	Returns to Interface configuration mode.
Step 3	`Router(config-if)# atm esi-address esi.selector`	Enters the ESI and selector fields of the NSAP address.

```
Router(config-if)# pvc 0/16 ilmi
Router(config-if-atm-vc)# exit
Router(config-if)# atm esi-address 3456.7890.1234.12
```

The recommended vpi value for the ILMI PVC is 0 and the recommended vci value is 16.

You can also specify a keepalive interval for the ILMI PVC.

Configuring the Complete NSAP Address

When you configure the ATM NSAP address manually, you must enter the entire address in hexadecimal format because each digit entered represents a hexadecimal digit. To represent the complete NSAP address, you must enter 40 hexadecimal digits in the following format:

```
XX.XXXX.XX.XXXXXX.XXXX.XXXX.XXXX.XXXX.XXXX.XXXX.XX
```

Note All ATM NSAP addresses may be entered in the dotted hexadecimal format shown, which conforms to the ATM Forum UNI specification. The dotted method provides some validation that the address is a legal value. If you know your address format is correct, the dots may be omitted.

Because the interface has no default NSAP address, you must configure the NSAP address for SVCs. To set the ATM interface source NSAP address, perform this task in interface configuration mode:

Command	Purpose
`Router(config-if)# atm nsap-address nsap-address`	Configures the ATM NSAP address for an interface.

This example shows how to configure the NSAP address:

```
Router(config-if)# atm nsap-address BC.CDEF.01.234567.890A.BCDE.F012.3456.7890.1334.13
Router(config-if)#
```

The **atm nsap-address** and **atm esi-address** commands are mutually exclusive. Configuring the router with the **atm nsap-address** command negates the **atm esi-address** setting and vice versa. You can display the ATM address for the interface by executing the **show interface atm** command.

Creating an SVC

To create an SVC, perform this task in interface configuration mode:

	Command	Purpose
Step 1	`Router(config-if)# svc [name] nsap address`	(Optional) Creates an SVC and specifies the destination NSAP address.
Step 2	`Router(config-if-atm-vc)# encapsulation {aal5mux | aal5snap}`	(Optional) Configures the ATM adaptation layer (AAL) and encapsulation type. The default is **aal5snap**.
Step 3	`Router(config-if-atm-vc)# protocol protocol protocol-address [[no] broadcast]`	Maps a protocol address to an SVC.

After you specify a name for an SVC, you can reenter interface-ATM-VC configuration mode by entering the **svc** *name* command; you can remove an SVC configuration by entering the **no svc** *name* command.

For a list of AAL types and encapsulations supported for the *aal-encap* argument, refer to the **encapsulation aal5** command in the "ATM Commands" chapter of the *Cisco IOS Wide-Area Networking Command Reference*. The default is AAL5 with SNAP encapsulation.

This example shows how to create an SVC:

```
Router(config-if)# svc nsap BC.CDEF.01.234567.890A.BCDE.F012.3456.7890.1334.13
Router(config-if-atm-vc)# encapsulation aal5mux
Router(config-if-atm-vc)# protocol ip 1.1.1.5 broadcast
Router(config-if-atm-vc)#
```

Configuring Multipoint Bridging

Multipoint bridging enables point-to-multipoint bridging for ATM permanent virtual circuits (PVCs). This feature allows the use of multiple VCs per VLAN for bridging.

Multipoint bridging allows service providers to add support for Ethernet-based Layer 2 services to the proven technology of their existing ATM legacy networks. Customers can then use their current VLAN-based networks over the ATM cloud. This also allows service providers to gradually update their core networks to the latest Gigabit Ethernet optical technologies, while still supporting their existing customer base.

ATM interfaces use RFC 1483 bridging which provides an encapsulation method to allow the transport of Ethernet frames over each type of Layer 2 network.

Note RFC 1483 has been obsoleted and superseded by RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*. RFC 1490 has been obsoleted and superseded by RFC 2427, *Multiprotocol Interconnect over Frame Relay*. To avoid confusion, this document continues to use the original RFC numbers.

In Cisco IOS Release 12.2(18)SXE, multipoint bridging supports the following modes of operation:

- Raw (default)—Default bridging access mode, in which the bridged connection acts on and transmits bridge protocol data unit (BPDU) packets.
- Access—Access-only bridging access mode, in which the bridged connection does not act on or transmit BPDU packets.
- 802.1Q—Performs IEEE 802.1Q tagging to preserve the class of service (CoS) information from the Ethernet frames across the ATM network.
- 802.1Q Tunnel—IEEE 802.1Q tunneling mode, so that service providers can use one VLAN to support customers with multiple VLANs, as well as accept untagged frames.

Restrictions and Usage Guidelines

The following restrictions apply to the Multipoint Bridging feature:

- Supported only on Enhanced OSMs; non-enhanced OSMs are not supported.
- On ATM interfaces, only permanent virtual circuits (PVCs) are supported. Switched virtual circuits (SVCs) are not supported.
- Up to 10,000 bridged PVCs are supported per router.
- VLAN ID 1 is not available as a bridge domain for doing multipoint bridging.
- Multipoint bridging supports an absolute maximum of 60 VCs per each VLAN, and an absolute maximum number of VLANs per peer is 4096. We recommend configuring at most 30 VCs per VLAN, with at most 1024 VLANs per VC.
- Do not use the **range pvc** command with stateful switchover (SSO).

Prerequisites

The following prerequisites apply to multipoint bridging:

- VLANs must be manually added to the VLAN database, using the **vlan** command, to be able to use those VLANs in multipoint bridging.

- Cisco IOS Release 12.2(18)SXE, and later releases, have renamed the **bridge-vlan** command to **bridge-domain**, and have added options to support multipoint bridging. Existing configurations of the **bridge-vlan** command are automatically renamed to **bridge-domain** in the running-config when upgrading to Cisco IOS Release 12.2(18)SXE. Be sure to save the running-config to startup-config to make these changes permanent.

Configuring Multipoint Bridging for ATM Interfaces

This section describes how to configure multipoint bridging on ATM interfaces. You can configure multipoint bridging manually on individual PVCs, or you can configure a range of PVCs to configure all of the PVCs at one time. To perform either task or both, use the following procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vlan** {*vlan-id* | *vlan-range*}
4. **interface atm** *slot/port*
5. **no ip address**

Note It is not recommended to configure an IP address on a bridged interface.

6. **interface atm** *slot/port.subinterface* [**point-to-point** | **multipoint**]

Note Use the following two commands (**pvc** and **bridge-domain**) to create and configure PVCs individually. Repeat these commands as desired.

7. **pvc** [*name*] *vpi/vci*
8. **bridge-domain** *vlan-id* [**access** | **dot1q** | **dot1q-tunnel**] [**ignore-bpdu-pid**] [**split-horizon**]

Note Use the following two commands (**range pvc** and **bridge-domain**) to create and configure a range of PVCs. Repeat these commands as desired.

9. **range** [*range-name*] **pvc** [*start-vpi/*]*start-vci* [*end-vpi/*]*end-vci*

Note Do not use the **range pvc** command with stateful switchover (SSO).

10. **bridge-domain** *start-vlan-id* [**access** | **dot1q** | **dot1q-tunnel**] [**ignore-bpdu-pid**] [**increment**] [**split-horizon**]
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vlan** {*vlan-id* | *vlan-range*} **Example:** `Router(config)# vlan 2,5,10-12,20,25,4000`	Adds the specified VLAN IDs to the VLAN database and enters VLAN configuration mode. • *vlan-id*—Specifies a single VLAN ID. The valid range is from 2 to 4094. • *vlan-range*—Specifies multiple VLAN IDs, as either a list or a range. The *vlan-range* can contain a list of the VLAN IDs, separated either by a comma (,), dash (-), or both. **Note** You must manually enter a VLAN ID into the VLAN database before you can use that VLAN for multipoint bridging.
Step 4	**interface atm** *slot/port* **Example:** `Router(config)# interface atm 8/0`	Enters configuration mode for the specified ATM interface.
Step 5	**no ip address** **Example:** `Router(config-if)# no ip address`	Removes the IP address on the main interface.
Step 6	**interface atm** *slot/port.subinterface* [**point-to-point** | **multipoint**] **Example:** `Router(config-if)# interface atm 8/0.100`	(Optional) Enters configuration mode for the specified subinterface, assuming that you are using subinterfaces to organize the PVCs. • **point-to-point**—Creates a point-to-point connection. • **multipoint**—Allows multiple PVCs to use the same VLAN.
	Use the following two commands (**pvc** and **bridge-domain**) to create and configure PVCs individually. Repeat these commands as desired.	
Step 7	**pvc** [*name*] *vpi/vci* **Example:** `Router(config-if)#`	Configures a new ATM PVC with the specified VPI and VCI numbers: • *name*—(Optional) Descriptive name to identify this PVC. • *vpi/vci*—Virtual path identifier (vpi) and virtual channel identifier (VCI) for this PVC.

	Command or Action	Purpose
Step 8	**bridge-domain** *vlan-id* [*access* | **dot1q** | **dot1q-tunnel**] [**ignore-bpdu-pid**] [**split-horizon**] **Example:** `Router(config-if-atm-vc)#`	Enables RFC 1483 bridging to map a bridged VLAN to a PVC. The following options are supported: **Note** This command has additional options that are not supported in a multipoint bridging configuration. • *vlan-id*—Number of VLAN to be used in this bridging configuration. The valid range is from 2 to 4094 (but the VLAN ID must have been previously added to the VLAN database in Step 3). **Note** This is the default configuration; frames are not tagged with the dot1q header but STPs and BPDUs are transmitted. • **access**—Enables bridging access mode, so that the bridged connection does not act on or transmit BPDUs. • **dot1q**—(Optional) Terminates dot1q traffic. Also enables IEEE 802.1Q tagging to preserve the class of service (CoS) information from the Ethernet frames across the ATM network. Without this option, the CoS values are not preserved. • **dot1q-tunnel**—(Optional) Enables IEEE 802.1Q tunneling mode, so that service providers can use one VLAN to support customers with multiple VLANs, as well as accept untagged frames. **Note** The **access**, **dot1q**, and **dot1q-tunnel** options are mutually exclusive. If you do not specify any of these options, the connection operates in "raw" bridging access mode, which is similar to **access**, except that the connection does act on and transmit BPDU packets. • **ignore-bpdu-pid**—(Optional, ATM interfaces only) Ignores bridge protocol data unit (BPDU) PID and treats all BPDU packets as data packets to allow interoperation with ATM customer premises equipment (CPE) devices that do not distinguish BPDU packets from data packets. • **split-horizon**—(Optional) Enables RFC 1483 split-horizon mode to globally prevent bridging between PVCs in the same VLAN.

Note Previous software releases used the **atm bridge-enable** command to enable ATM RFC 1483 bridging, but Cisco IOS Release 12.2(18)SXE and later 12.2 SX releases have deprecated this command for OSM interfaces.

Note Use the following two commands (**range pvc** and **bridge-domain**) to create and configure a range of PVCs. Repeat these commands as desired.

Note Do not use the **range pvc** command with stateful switchover (SSO).

	Command or Action	Purpose
Step 9	**range** [*range-name*] **pvc** [*start-vpi/*]*start-vci* [*end-vpi/*]*end-vci* **Example:** `Router(config-if-atm-vc)# range pvc 1/121 1/180`	Creates a range of PVCs, and enters PVC range configuration mode: • *range-name*—(Optional) Descriptive name of the range, up to a maximum of 15 characters. • *start-vpi/*—(Optional) Beginning value for the range of virtual path identifiers (VPIs). The valid range is from 0 to 255, with a default of 0. • *start-vci*—Beginning value for a range of virtual channel identifiers (VCIs). The valid range is from 32 to 65535. • *end-vpi*—End value for the range of VPIs. The valid range is from 0 to 255, with a default that is equal to the start-vpi value. • *end-vci*—End value for a range of virtual channel identifiers (VCIs). The VCI value ranges from 32 to 65535.

Step 10	**bridge-domain** *vlan-id* [**access** | **dot1q** | **dot1q-tunnel**] [**ignore-bpdu-pid**] [**increment**] [**split-horizon**]
	
	Example:
	`Router(config-if-atm-range)# bridge-domain 121 increment`
	`Router(config-if-atm-range)#`
		Enables RFC 1483 bridging to map a bridged VLAN to the configured range of PVCs. In addition to the options that are shown in Step 8, this command supports the following option when used in PVC range configuration mode:
		• **increment**—Increments the bridge domain number for each PVC in the range.

Step 11	**end**
	
	Example:
	`Router(config-if-atm-range)# end`
	`Router#`
		Exits VC or PVC range configuration mode and returns to privileged EXEC mode.

The following example shows both a range of PVCs and an individual PVC being configured for multipoint bridging:

```
interface ATM3/1.101 multipoint
 range pvc 102/100 102/102
  bridge-domain 102 increment
 !
 mls qos trust dscp
```

Verification

To display information about the PVCs that have been configured on ATM interfaces, use the following commands:

- **show atm pvc**—Displays a summary of the PVCs that have been configured.
- **show atm vlan**—Displays the connections between PVCs and VLANs.

Tip Use the **show atm vlan** command instead of the **show interface trunk** command to display information about ATM interfaces being used for multipoint bridging.

The following shows an example of each command:

```
Router# show atm pvc
           VCD /                                          Peak  Avg/Min Burst
Interface  Name          VPI   VCI  Type   Encaps   SC   Kbps   Kbps   Cells  Sts
3/1.100    3             101   100  PVC    SNAP     UBR  599040                UP
3/1.100    4             111   100  PVC    SNAP     UBR  599040                UP
3/2.100    3             102   100  PVC    SNAP     UBR  599040                UP
3/2.100    4             112   100  PVC    SNAP     UBR  599040                UP

Router# show atm vlan

 Options Legend: DQ - dot1q;  DT - dot1q-tunnel;  MD - multi-dot1q;
                 AC - access; SP - split-horizon; BR - broadcast;
                 IB - ignore-bpdu-pid;
                 DEF - default

Interface              VCD    VPI      Network   Customer   PVC     Options
                              /VCI     Vlan ID   Dot1Q-ID   Status

ATM3/1.100              3   101/100       101        -        UP    DEF
ATM3/1.100              4   111/100       111        -        UP    DEF
ATM3/2.100              3   102/100       102        -        UP    DEF
ATM3/2.100              4   112/100       112        -        UP    DEF
```

RFC 1483 Spanning-Tree Interoperability Enhancements

The RFC 1483 Spanning-Tree Interoperability Enhancements feature allows interoperability between two different BPDU formats (PVST+ and 802.1d) between Cisco 7600 series routers and legacy Catalyst 5500 ATM switches, Cisco 7200 routers, and Cisco 7500 routers.

This section describes an interoperability feature for the various Spanning-Tree implementations across 1483 Bridge-Mode ATM PVCs. Historically, vendors have not implemented Spanning-Tree across 1483 encapsulation consistently; furthermore, some Cisco IOS versions may not support the full range of Spanning-Tree options. This feature attempts to smooth some of the practical challenges of interworking common variations of Spanning-tree over RFC 1483 Bridged-Mode encapsulation.

Note This feature set is only supported on RFC 1483 Bridged-Mode ATM PVCs.

Let's first define the basic terms:

- *IEEE 802.1D* is a standard for interconnecting LANs through MAC bridges (see Figure 8-4 on page 8-21). 802.1D uses the Spanning-Tree Protocol to eliminate loops in the bridge topology, which cause broadcast storms.
- *Spanning-Tree Protocol (STP)* as defined in the IEEE 802.1D is a link management protocol that provides path redundancy while preventing undesirable loops in the network. An IEEE 802.1D spanning tree makes it possible to have one Spanning Tree instance for the whole switch, regardless of the number of VLANs configured on the switch.
- *Bridge Protocol Data Unit (BPDU)* is the generic name for the frame used by the various spanning-tree implementations. The Spanning-Tree Protocol uses the BPDU information to elect the root switch and root port for the switched network, as well as the root port and designated port for each switched segment.

- *Per VLAN Spanning Tree (PVST)* is a Cisco proprietary protocol that allows a Cisco device to support multiple spanning tree topologies on a per-VLAN basis. PVST uses the BPDUs defined in IEEE 802.1D (see Figure 8-4 on page 8-21), but instead of one STP instance per switch, there is one STP instance per VLAN.
- *PVST+* is a Cisco proprietary protocol that creates one STP instance per VLAN (as in PVST). However, PVST+ enhances PVST and uses Cisco proprietary BPDUs with a special 802.2 SNAP OUI (see Figure 8-2 on page 8-20) instead of the standard IEEE 802.1D frame format used by PVST (see Figure 8-4). PVST+ BPDUs are also known as SSTP (Shared Spanning Tree Protocol) BPDUs.

Note RFC 1483 is referenced throughout this section, although it has been superseded by RFC 2684.

Supported Supervisors and Line Cards

The Cisco 7600 router supports PVST to PVST+ BPDU interoperability with the following Supervisors and line cards:

Supervisor 720 Line Cards

- Enhanced FlexWAN
- FlexWAN
- 7600 SIP-200
- ATM Optical Services Module (OSM)

Supervisor 2 Line Cards

- Enhanced FlexWAN
- FlexWAN
- ATM Optical Services Module (OSM)

Prerequisites

The RFC 1483 Spanning-Tree Interoperability Enhancements feature requires Cisco IOS Release 12.2(18)SXF1 or later.

The Interoperability Problem Summarized

The current interoperability problem can be summarized as follows:

- When transmitting STP BPDUs, many vendors' implementations of ATM-to-Ethernet bridging are not fully compliant with the specifications of RFC 1483, Appendix B. The most common variation of the standard is to use an ATM Common Part Convergence Sublayer (CPCS) SNAP PDU with OUI: 00-80-C2 and PID: 00-07. Appendix B reserved this OUI/PID combination for generic Ethernet frames without BPDUs. Appendix B specifies OUI: 00-80-C2, PID: 00-0E for frames with BPDU contents.
- There are several varieties of the Spanning-Tree protocol used by Cisco products on ATM interfaces. The Catalyst 5000 supports only PVST on ATM interfaces. The Cisco 7600 and Catalyst 6500 support only PVST+ on ATM interfaces. Most other Cisco routers implement classic IEEE 802.1D on ATM interfaces.

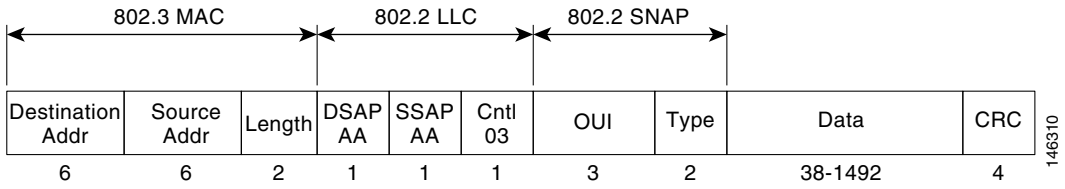
When the Cisco 7600 router and the Catalyst 6500 switch first implemented 1483 Bridging (on Cisco IOS 12.1E) on the Cisco 7600 FlexWAN module, the platform uses OUI: 00-80-C2 and PID: 00-0E to maximize interoperability with all other Cisco IOS products.

However, there are so many implementations that do not send PVST or 802.1D BPDUs with PID: 00-0E that the Cisco 7600 and the Catalyst 6500 reverted to the more common implementation of RFC 1483 (with PID: 00-07) in Cisco IOS 12.2SX. This feature provides the option of encapsulating BPDUs across 1483 with either PID: 00-07 or PID: 00-0E.

BPDU Packet Formats

In this section, the various BPDU packet formats are described. Figure 8-2 shows the generic IEEE 802.2/802.3 frame format, which is used by PVST+—but is not used by PVST.

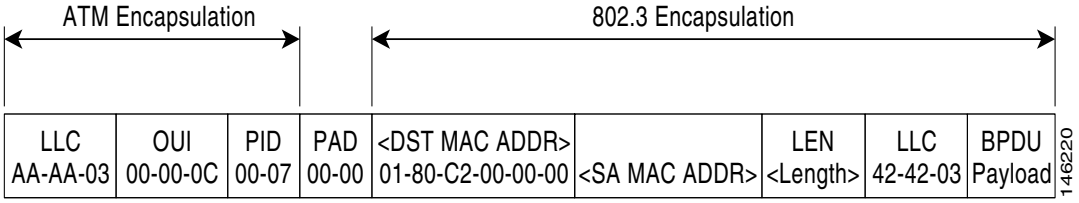
Figure 8-2 IEEE 802.2/802.3 SNAP Encapsulation (RFC 1042)



Catalyst 5000 PVST BPDU Packet Format

The Catalyst 5000 Series switches send and receive BPDUs in PVST format on ATM interfaces (see Figure 8-3):

Figure 8-3 BPDU PVST Frame Used by the Catalyst 5000 Switch



BPDUs sent by the Catalyst 5000 use a PID of 0x00-07, which does not comply with RFC1483. The Cisco 7600 router also has the ability to send BPDUs in this data format.

By using the **bridge-domain** command's **ignore-bpdu-pid** optional keyword, the Catalyst 5000 switch sends this frame by default.

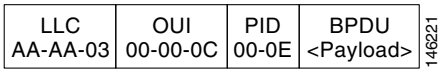
The Catalyst 5000 cannot accept the PVST+ BPDUs and blocks the ATM port, giving the following error message:

```
%SPANTREE-2-RX_1QNON1QTRUNK: Rcved 1Q-BPDU on non-1Q-trun port 6/1 vlan 10
%SPANTREE-2-RX_BLKPORTPVID: Block 6/1 on rcving vlan 10 for inc peer vlan 0
```

Cisco 7200/7500 IEEE BPDU Frame Format

Figure 8-4 shows the Cisco 7200/7500 routers IEEE BPDU frame format:

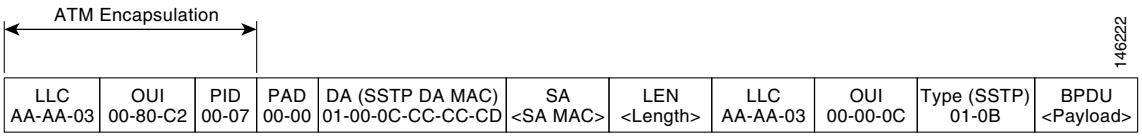
Figure 8-4 Frame Format for the Cisco 7200/7500 IEEE BPDU



Cisco 7600 PVST+ BPDU Frame Format

The Cisco 7600 router PVST+ BPDU packet format is as shown in Figure 8-5. These BPDUs are not IEEE BPDUs, but Cisco proprietary SSTP BPDUs.

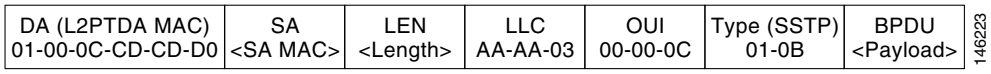
Figure 8-5 Cisco 7600 PVST+ BPDU Frame (1483 Bridged)



Cisco L2PT BPDU Frame Format

Figure 8-6 shows the Cisco Layer 2 Protocol Tunneling (L2PT) BPDU SNAP frame format:

Figure 8-6 L2PT BPDU SNAP Frame Format



BPDU Translation Command Line Interface Summary

In order to resolve the interoperability problem as described in the previous section, Cisco has introduced the following new keywords for the **bridge-domain** command:

- **ignore-bpdu-pid**
- **pvst-tlv**

The ignore-bpdu-pid Keyword

Without the **ignore-bpdu-pid** keyword, the permanent virtual circuit (PVC) between the devices operates in an RFC 1483 compliant manner, which is referred to as *strict mode*. Using the **ignore-bpdu-pid** keyword is known as *loose mode*.

- Without this keyword, IEEE BPDUs are sent out using a PID of 0x00-0E, which complies with RFC 1483.

- With this keyword, IEEE BPDUs are sent out using a PID of 0x00-07, which is normally reserved for 1483 data.

  For details, refer to the "BPDU Packet Formats" section on page 8-20.

Cisco proprietary PVST+ BPDUs are always sent out on data frames using a PID of 0x00-07, regardless of whether the **ignore-bpdu-pid** keyword is used.

Use the **<ignore>** keyword when connecting to devices that send PVST (or 802.1D) BPDUs with PID: 00-07. This includes the vast majority of CPE devices, such as ATM DSL modems.

The pvst-tlv Keyword

The **pvst-tlv** keyword enables BPDU translation when interoperating with devices that understand only PVST or IEEE Spanning Tree Protocol. Since the Cisco 7600 ATM modules support PVST+ only, the **pvst-tlv** keyword must be used when connecting to a Catalyst 5000 switch, which only understands PVST on its ATM modules, or when connecting with other Cisco IOS routers, which understand IEEE format only.

- When transmitting, the **pvst-tlv** keyword translates PVST+ BPDUs into IEEE BPDUs.
- When receiving, the **pvst-tlv** keyword translates IEEE BPDUs into PVST+ BPDUs.

When a Cisco 7600 Router Is Connected to a Cisco 7200 Router

For example, the Cisco 7200 router is a device that only understand IEEE BPDUs in an RFC 1483 compliant manner. Thus, when a Cisco 7600 router is connected to a Cisco 7200 router, the keywords used should be as follows:

```
bridge-domain <vlan> pvst-tlv <vlan>
```

The **ignore-bpdu-pid** keyword is not used in this case because the Cisco 7200 router must operate in an RFC 1483 compliant manner for IEEE BPDUs.

When a Cisco 7600 Router Is Connected to a Catalyst 5500 ATM Module

The Catalyst 5500 ATM module is a device that only understands PVST BPDUs in a non-RFC1483 compliant manner. Therefore, when a Cisco 7600 router is connected to a Catalyst 5500 ATM module, we need to use both keywords:

```
bridge-domain <vlan> ignore-bpdu-pid pvst-tlv <vlan>
```

Layer 2 Protocol Tunneling Topology CLI

To enable BPDU translation for the Layer 2 Protocol Tunneling (L2PT) topologies, use the following command line:

```
bridge-domain <PE vlan> dot1q-tunnel ignore-bpdu-pid pvst-tlv <CE vlan>
```

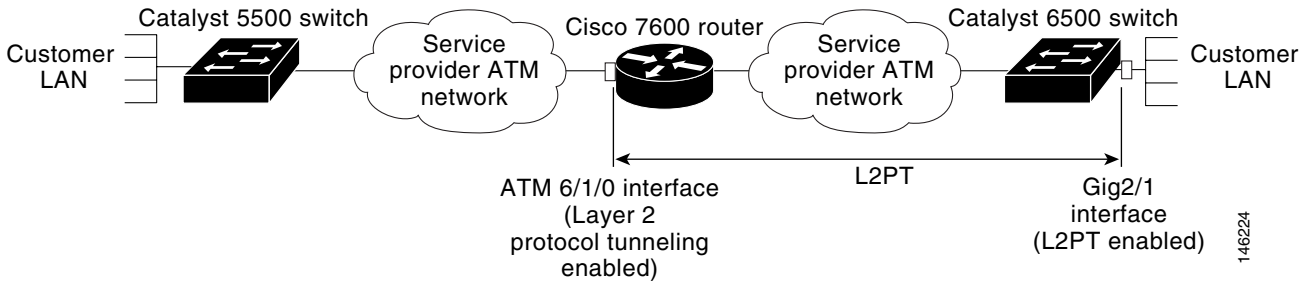
Typical Topologies Requiring BPDU Translation

This section describes the most common network scenarios and provides the configuration commands necessary to enable BPDU translation between the devices in each example.

Layer 2 Protocol Tunneling Topology with a Cisco 7600, Catalyst 5500, and Catalyst 6500

Figure 8-7 shows one sample network topology in which data packets are sent between a Catalyst 5500 switch and a Cisco 7600 router:

Figure 8-7 Catalyst 5500 Switch and Cisco 7600 Routers in an L2PT Topology



As shown in Figure 8-7, Layer 2 Protocol Tunneling (L2PT) is configured at the Cisco 7600 ATM6/1/0 interface and also at the Catalyst 6500 Ethernet2/1 interface.

PVST packets are sent from the Catalyst 5500 switch to the Cisco 7600 router. The Cisco 7600 router transports those BPDUs via L2PT and sends them to the Catalyst 6500. Those BPDUs are decapsulated and restored before sending the packets out to the customer network.

Assume that the 7600 and the Catalyst 6500 are PE devices and the rest are CE devices.

ATM Configuration Example

Any traffic coming in must be sent via a dot1q-tunnel. Assuming the PE-VLAN is 200 and the CE-VLAN is 100, we have the following configuration:

```
Router(config)#int atm 6/1/0
Router(config-if)#pvc 6/200
Router(config-if-atm-vc)#bridge-domain 200 dot1q-tunnel ignore-bpdu-pid pvst-tlv 100
Router(config-if-atm-vc)#
```

Ethernet Configuration Example

The Ethernet configuration is something like this:

```
Router(config)#int gig2/1/0
Router(config-if)#switchport
Router(config-if)#switchport access vlan 200
Router(config-if)#switchport mode dot1q-tunnel
Router(config-if)#l2protocol-tunnel
```

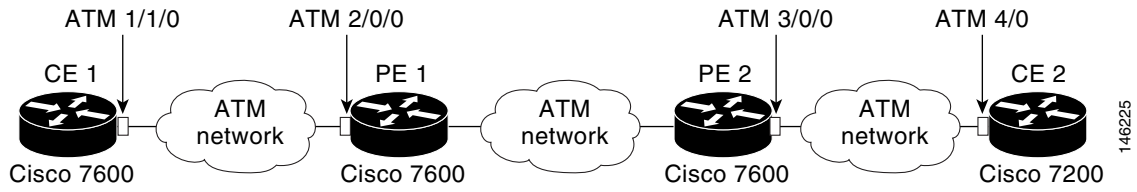
CE-VLAN 100 is what is used at the customer sites. The Catalyst 5500 sends the IEEE BPDU in data format. The Cisco 7600 router receives the BPDU and first converts it to PVST+ format. Then the DA MAC of the frame is changed to the protocol tunnel MAC address and sent out into the Layer 2 cloud.

At the other end, when the frame leaves the gige2/1/0 interface, the DA MAC is changed back to the PVST+ DA MAC and the PVST+ BPDU is sent to the CPE device.

Layer 2 Protocol Tunneling Topology with a Cisco 7600 and Cisco 7200

In the example shown in Figure 8-8, a Cisco 7600 router needs to communicate with a Cisco 7200 router:

Figure 8-8 Cisco 7600 and Cisco 7200 Routers in an L2PT Topology



PE Configuration

On the PEs, the configuration looks something like this:

```
!On PE 1
interface ATM2/0/0
    no ip address
    atm mtu-reject-call
    pvc 7/101
    bridge-domain 200 dot1q-tunnel
    !
end
!On PE 2
interface ATM3/0/0
    no ip address
    pvc 2/101
    bridge-domain 200 dot1q-tunnel pvst-tlv 100
    !
end
```

Cisco 7600 CE Configuration

The configuration for the Cisco 7600 CE 1 would be as follows:

```
!On CE 1
interface ATM1/1/0
    no ip address
    atm mtu-reject-call
    pvc 7/101
    bridge-domain 101
    !
end
```

Cisco 7200 CE Configuration

The configuration for the Cisco 7200 (CE 2) router would be like this:

```
!On CE 2
interface ATM4/0
    no ip address
    no atm ilmi-keepalive
    pvc 2/101
    !
    bridge-group 101
end
```

Data Transmission Sequence from the Cisco 7200 CE to the Cisco 7600 CE

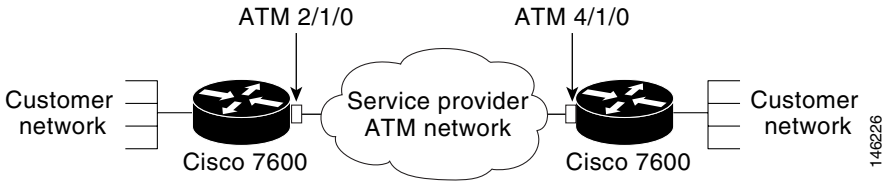
Given the configurations and topologies summarized here, the data transmission sequence from the Cisco 7200 CE to the Cisco 7600 CE is as follows:

1. The Cisco 7200 CE 2 sends BPDUs without the MAC header in RFC1483 format.
2. The Cisco 7600 PE receives it and then translates the IEEE BPDU into PVST+ BPDU format.
3. VLAN 100 is inserted into the PVST+ BPDU.
4. Then the frame's DA MAC is rewritten to use the protocol tunnel destination address (DA) MAC and is sent out into the ATM network cloud.
5. The L2PT BPDU needs to go out of PE 1's ATM2/0/0 interface. The DA MAC is restored to the PVST+ DA MAC.
6. Finally, the PVST+ BPDU is sent to the 7600 CE 1 device.

7600 Basic Back-to-Back Scenario

The basic back-to-back scenario in Figure 8-9 is as follows:

Figure 8-9 Cisco 7600 Routers in Basic Back-to-Back Topology



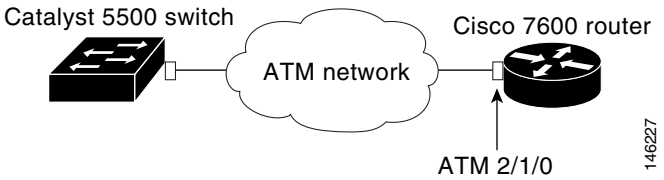
The PDUs exchanged are PVST+ BPDUs. The PVST+ BPDUs are sent using a PID of 0x0007. Here is the configuration:

```
Router(config)#int atm 2/1/0
Router(config-if)#pvc 2/202
Router(config-if-atm-vc)#bridge-domain 101
Router(config-if-atm-vc)#
```

Catalyst 5500 Switch and Cisco 7600 Routers in Back-to-Back Topology

Another sample topology, shown in Figure 8-10, is a simple back-to-back setup, which serves to test basic Catalyst 5500 and Cisco 7600 interoperability.

Figure 8-10 Catalyst 5500 Switch and Cisco 7600 Routers in Back-to-Back Topology



When connected to a device that sends and receives IEEE BPDUs in data format (PID 0x0007) like the Catalyst 5000's ATM module, the configuration must be something like this:

```
Router(config)#int atm 2/1/0
Router(config-if)#pvc 2/202
```

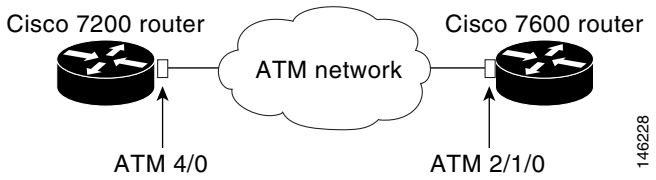
```
Router(config-if-atm-vc)#bridge-domain 101 ignore-bpdu-pid pvst-tlv 101
Router(config-if-atm-vc)#
```

The Cisco 7600 router translates its outgoing PVST+ BPDUs into IEEE BPDUs. Because the **ignore-bpdu-pid** keyword is also enabled, it uses a PID of 0x0007, which is exactly what the Catalyst 5500 switch expects.

Cisco 7600 and Cisco 7200 in Back-to-Back Topology

When connecting to a device that is completely RFC1483 compliant, in which the IEEE BPDUs are sent using a PID of 0x000E, you must use the new **ignore-bpdu-pid** keyword in the **bridge-domain** command.

Figure 8-11 Cisco 7600 Router and Cisco 7200 Router in Back-to-Back Topology



For example, when a Cisco 7600 is connected to a Cisco 7200 router, you would have this configuration:

```
Router(config)#int atm 2/1/0
Router(config-if)#pvc 2/202
Router(config-if-atm-vc)#bridge-domain 101 pvst-tlv 101
Router(config-if-atm-vc)#
```

Note In this case, the CE-VLAN must be the same as the bridge-domain VLAN.

Configuring Automatic Protection Switching

The Automatic Protection Switching (APS) feature supports Linear 1+1 APS as described in section 5.3 of the Telcordia publication"*GR-253-CORE SONET Transport Systems: Common Generic Criteria*."

Linear APS is defined to provide protection at the line layer. All of the STS synchronous payload envelopes (SPEs) carried in an OC-N signal are protected so that if a protection switch occurs, all of the VCs are switched simultaneously.

One port on an OC-12 ATM OSM can be protected by:

- Another port on the same OC-12 ATM OSM
- A different port on another OC-12 ATM OSM in the same router
- A different port on another OC-12 ATM OSM in a different router

Note Installing APS in different routers to protect against router failure requires that you update the protect interface with the current VC context of the working interface. To accomplish this, you must configure the VC configuration on the protect interface manually.

When configuring APS, we recommend that you configure the working interface first, along with the IP address of the interface being used as the APS OOB communication path.

Note To prevent the protected interface from becoming the active circuit and disabling the working circuit when it is discovered, configure the working interface before configuring the protected interface.

For more information on APS and configuration information for additional APS features, refer to the *Cisco IOS Interface Configuration Guide,* Release 12.1 at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/inter_c/index.htm

Configuring the Working Interface

To configure the working interface, perform this task:

Note A typical ATM interface configuration contains several subinterfaces with each having a different IP address and VCs. When configuring a protect interface, ensure that it contains same VCs as the working interface. Because the IP address cannot be the same on two interfaces, the IP addresses you configure on the protect interface should be in same subnet.

	Command	Purpose
Step 1	`Router(config)# interface atm slot/port`	Specifies an ATM interface and enters interface configuration mode.
Step 2	`Router(config-controller)# aps working circuit-number`	Configures this interface as a working interface.
Step 3	`Router(config)# end`	Exits configuration mode.

Step 4	`Router# show controllers atm`
	`Router# show interface atm`
	`Router# show aps`
	`Router# show aps controller`
		Displays information about the ATM controllers and interface so that you can verify that the interface is configured correctly.

Note If a router has two or more protect interfaces, the **aps group** command for each interface must precede the corresponding **aps protect** command.

Configuring the Protect Interface

To configure the protect interface, perform this task beginning in global configuration mode:

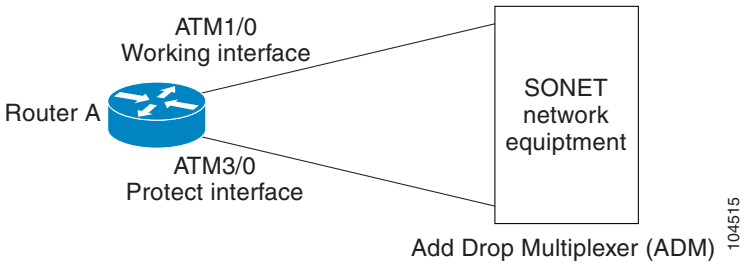
	Command	Purpose
Step 1	`Router(config)# interface atm slot/port`	Specifies an ATM interface and enters interface configuration mode.
Step 2	`Router(config-if)# aps protect circuit-number ip-address`	Configures this interface as a protect interface. Specifies the IP address of the router that contains the working interface.
Step 3	`Router(config-if)# end`	Exits configuration mode.

Step 4	`Router# show controllers atm`
	`Router# show interface atm`
	`Router# show aps`
		Displays information about the ATM controllers and interface so that you can verify that the interface is configured correctly.

Configuring Basic APS on a Single Router

Figure 8-12 shows the configuration of APS on router A and router B. Router A has both the working and protect interfaces. If the working interface ATM1/0 becomes unavailable, the connection automatically switches over to the protect interface ATM3/0. Single router APS configuration is typically used to protect line card failures.

Figure 8-12 Basic Single Router APS Configuration



Step 1 Configure a loopback interface on Router A:

```
RouterA# configure terminal
RouterA(config)# interface Loopback 0/0
RouterA(config-if)# ip address 7.7.7.7 255.255.255.255
RouterA(config-if)# end
RouterA#
```

Step 2 Configure the working and protect interfaces on router A:

```
RouterA# configure terminal
RouterA(config)# interface ATM 1/0
RouterA(config-if)# aps working 1
RouterA(config-if)# exit
RouterA(config)# interface ATM 3/0
RouterA(config-if)# aps protect 1 7.7.7.7
RouterA(config-if)# end
```

Step 3 Configure VCs on both working and protect interfaces:

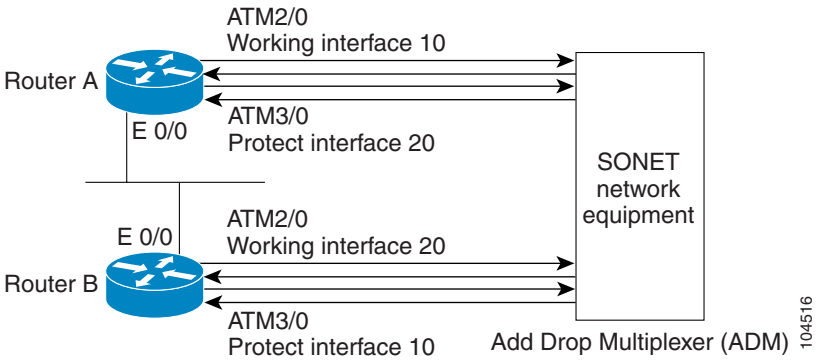
```
RouterA# configure terminal
RouterA(config)# int atm 1/0.1 point-to-point
RouterA(config-subif)# ip address 10.1.1.1 255.255.255.0
RouterA(config-subif)# pvc 0/100
RouterA(config-subif)# exit
RouterA(config)# int atm 3/0.1 point-to-point
RouterA(config-subif)# ip address 10.1.1.1 255.255.255.0
RouterA(config-subif)# pvc 0/100
RouterA(config-subif)# exit
RouterA(config)# end
RouterA#
```

Note Because APS protocol provides redundancy on the line (not end to end), you must configure a duplicate IP address on the protect interface. There is no automatic configuration of the protect interface. You must manually configure all of the VCs that require redundancy on the protect interface.

Basic Multiple Router APS Configuration

Figure 8-13 shows the configuration of APS on router A and router B. Router A is configured with the working interface and router B is configured with the protect interface. If the working interface on router A becomes unavailable, the connection automatically switches over to the protect interface on router B. This is typically used to protect against both line card and router failures.

Figure 8-13 Basic Multiple Router APS Configuration



Step 1 Configure the working interface on RouterA:

```
RouterA# configure terminal
RouterA(config)# interface ethernet 0/0
RouterA(config-if)# ip address 7.7.7.7 255.255.255.0
RouterA(config-if)# exit
RouterA(config)# interface ATM 1/0
RouterA(config-if)# aps working 1
RouterA(config-if)# end
RouterA#
```

Step 2 Configure the protect interfaces on router B:

```
RouterB# configure terminal
RouterB(config)# interface ethernet 0/0
RouterB(config-if)# ip address 7.7.7.6 255.255.255.0
RouterB(config)# interface ATM 3/0
RouterB(config-if)# aps protect 1 7.7.7.7
RouterB(config-if)# end
RouterB#
```

Step 3 Configure the VCs on router A:

```
RouterA# configure terminal
RouterA(config)# int atm 1/0.1 point-to-point
RouterA(config-subif)# ip address 10.1.1.1 255.255.255.0
RouterA(config-subif)# pvc 0/100
RouterA(config-subif)# exit
RouterA(config)# end
RouterA#
```

Step 4 Configure the same VCs on router B:

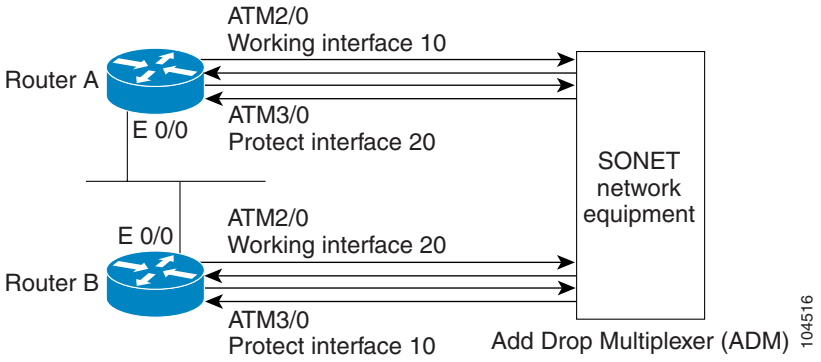
```
RouterB# configure terminal
RouterB(config)# int atm 3/0.1 point-to-point
RouterB(config-subif)# ip address 10.1.1.1 255.255.255.0
RouterB(config-subif)# pvc 0/100
```

```
RouterB(config-subif)# exit
RouterB(config)# end
RouterB#
```

Multiple APS Interface Configuration

To configure more than one protect/working interface on a router, use the **aps group** command. Figure 8-14 shows the configuration for grouping more than one working/protect interface on a router. Both router A and B are configured with a working interface and a protect interface. If the working interface 2/0 on router A becomes unavailable, the connection switches over to the protect interface 3/0 on router B because they are both in APS group 10. Similarly, if the working interface 2/0 on router B becomes unavailable, the connection switches over to the protect interface 3/0 on router A because they are both in APS group 20.

Figure 8-14 Multiple APS Interface Configuration



Note Before you configure the protected interface, configure the working interface to avoid the protected interface from becoming the active circuit and disabling the working circuit when it is discovered.

Step 1 On router A, which contains the working interface for group 10 and the protect interface for group 20, use the following configuration:

```
RouterA# configure terminal
RouterA(config)# interface ethernet 0/0
RouterA(config-if)# ip address 7.7.7.6 255.255.255.0
RouterA(config)# interface ATM2/0
RouterA(config)# aps group 10
RouterA(config-if)# aps working 1
RouterA(config)# interface ATM3/0
RouterA(config-if)# aps group 20
RouterA(config-if)# aps protect 1 7.7.7.7
RouterA(config-if)# end
RouterA#
```

Step 2 On router B, which contains the protect interface for group 10 and the working interface for group 20, use the following configuration:

```
RouterB# configure terminal
RouterB(config)# interface ethernet 0/0
RouterB(config-if)# ip address 7.7.7.7 255.255.255.0
RouterB(config)# interface ATM2/0
RouterB(config)# aps group 20
RouterB(config-if)# aps working 1
```

```
RouterB(config)# interface ATM3/0
RouterB(config-if)# aps group 10
RouterB(config-if)# aps protect 1 7.7.7.6
RouterB(config-if)# end
RouterB#
```

APS Commands

The commands below are applicable to APS with ATM. For information on using these commands, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/cc111/posaps.htm#xtocid13.

Note Be sure you change the interface from POS to ATM when using these commands with ATM.

- aps authenticate
- aps force
- aps group
- aps lockout
- aps manual
- aps protect
- aps revert
- aps timers
- aps unidirectional
- aps working
- show aps

SONET and SDH Configuration Commands

The default framing on the 2-port OC-12 ATM OSMs is SONET, but the modules also support SDH. Use the following commands to change the mode of operation, specify the BER threshold values, and enable alarm reporting.

atm framing sonet | sdh

Use the **atm framing sonet | sdh** command to specify the framing. The default framing is SONET.

```
Router(config-if)# atm framing sdh
Router(config-if)#
```

atm sonet stm-4

Use the **atm sonet stm-4** interface configuration command to set the mode of operation and control the type of ATM cell used for cell-rate decoupling on the SONET physical layer interface module (PLIM). The **no** form of this command restores the default Synchronous Transport Signal level 12 (STS-12c) operation.

Note The **atm sonet stm-4** and **atm framing sdh** commands both change the framing to SDH. The commands are functionally identical.

[no] atm sonet stm-4

This example shows how to change the mode from STS-12 to STM-4 and verify the configuration:

```
Router(config-if)# atm sonet stm-4
Router(config-if)# end
Router# show controllers atm 3/1
Interface ATM3/1 is up

hwidb addr:42773F94, instance addr:42780F64

Framing mode:SDH (STM-4)
Clock source:Line

VPIs in use:3, max VPIs:15

  VPI  # VCs      VPI  # VCs      VPI  # VCs
  ---  -----      ---  -----      ---  -----
    0    201        1      3      255      1

ATM framing errors:
  HCS (correctable):  1058413
  HCS (uncorrectable):3851467
  LCD:                18

SONET Subblock:
SECTION
  LOF = 0          LOS =    2          RDOOL = 0          BIP(B1) = 1020363
  Active Alarms:None
  Active Defects:None
  Alarm reporting enabled for:LOF LOS B1-TCA
LINE
  AIS = 0          RDI =    5          FEBE =  437717490  BIP(B2) = 457516655
  Active Alarms:None
  Active Defects:None
  Alarm reporting enabled for:B2-TCA SF
PATH
  AIS = 0          RDI =    13         FEBE =  345027     BIP(B3) = 1229383
  LOP = 2          NEWPTR = 0          PSE =   0          NSE =     0
  Active Alarms:None
  Active Defects:None
  Alarm reporting enabled for:LOP B3-TCA

BER thresholds: SF = 10e-3, SD = 10e-6
TCA thresholds: B1 = 10e-6, B2 = 10e-6, B3 = 10e-6
Router#
```

atm sonet report

Use the **atm sonet report** interface configuration command to set the ATM SONET alarm reporting. The **no** form of this command removes the alarm reporting.

[**no**] **atm sonet report** {**all** | **b1-tca** | **b2-tca** | **b3-tca** | **default** | **lais** | **lrdi** | **pais** | **plop** | **pplm** | **prdi** | **ptim** | **puneq** | **sd-ber** | **sf-ber** | **slof** | **slos**}

This example shows how to enable alerts for B1 threshold crossings:

```
Router(config-if)# atm sonet report b1-tca
Router(config-if)#
```

atm sonet threshold

Use the **atm sonet threshold** interface configuration command to set the BER threshold values. Use the **no** form of the command to remove the configuration:

[**no**] **atm sonet-threshold** {**b1-tca** *value* | **b2-tca** *value*| **b3-tca** *value*| **sd-ber** *value*| **sf-ber** *value*}

This example shows how to set the B1 threshold:

```
Router(config-if)# atm sonet threshold b1-tca 9
Router(config-if)#
```

show controllers atm

Use the **show controllers atm** command to display information about physical port hardware information.

show controllers atm [***slot****/port-adapter/port*]

This example shows how to show the output for an OC-12ATM linecard.

```
Router# show controllers atm 6/1
```

The output of this command is as follows:

```
~~~~~~~~~
btaps2#sh cont atm 6/1
Interface ATM6/1 is up
hwidb: 0x4316B388, instance: 0x4316EC30, 5 i/f transitions
Framing mode: SONET (STS-12c) Clock source: Internal -- Reason: Configured
VPIs in use: 0, max VPIs: 15
ATM framing errors:
  HCS (correctable):   8
  HCS (uncorrectable): 4375
  LCD:                 0

SONET Subblock:
APS                          <============APS info displayed...
  COAPS = 0          PSBF = 0
  State: PSBF_state = false
  Rx(K1/K2): 0 /0   Tx(K1/K2): 0 /5
SECTION
  LOF = 0          LOS = 0                              BIP(B1) = 65
LINE
  AIS = 0          RDI =    0          FEBE =  712        BIP(B2) = 0
PATH
  AIS = 0          RDI =    1          FEBE =  65535      BIP(B3) = 134
```

```
  LOP = 0          NEWPTR = 0          PSE = 0           NSE = 0

Active Defects: None
Active Alarms:  None
Alarm reporting enabled for: SF SLOS SLOF B1-TCA B2-TCA PLOP B3-TCA

BER thresholds:  SF = 10e-3, SD = 10e-6
TCA thresholds:  B1 = 10e-6, B2 = 10e-6, B3 = 10e-6

Rx S1S0 = 00, Rx C2 = 13

PATH TRACE BUFFER : STABLE
  Remote hostname : btaps1
  Remote interface: ATM6/1
  Remote IP addr  : 0.0.0.0
  Remote Rx(K1/K2): 00/00  Tx(K1/K2): 00/00
~~~~~~~~
```